Anti-Money Laundering / Counter Terrorist Financing Policy

Al Rostamani International Exchange

Issued by: Risk & Compliance Department

Approved by: General Manager

Revision No.: 02, Revision date: 30 June 2016

Objective

The compliance to regulatory requirements and supporting efforts to combat money laundering and terrorist financing is a sustained emphasis within the Company, and is directed by top Management.

Through this Policy Document, Al Rostamani International Exchange (ARIE) wishes to convey it's position on AML/CTF, and reiterate that the Company shall conduct business operations in total compliance with all applicable laws, regulations and worldwide best practices in the area of AML/CTF. ARIE shall consider the fight against money laundering and/or counter terrorist financing as a priority for our organization and recognize it as a team effort.

ARIE shall support all the regulators globally such as FATF, OFAC, UN, EU and the local regulatory authority, namely the Central Bank of the UAE which collectively set and enforce standards for anti- money laundering and counter terrorist financing policies and programs.

ARIE shall maintain the highest operating standards to safeguard the interest of all stake holders including customers, shareholders, employees, our business partners and the jurisdiction in which we operate. This shall be accomplished through ongoing and continual development of staff members, use of upto date technology and Systems that support our efforts to combat money laundering and counter terrorist financing and other related financial crimes.

Employees of ARIE shall ensure that they adhere to the standards to comply with norms set forth by local as well as international regulatory authorities and to protect ARIE and its reputation from being misused for any illicit activity.

ARIE's AML/CTF policy/procedure applies to all its employees, regardless of their function or location of work. The operations of the Company are based in UAE and the Company does not have any branches or subsidiaries in any of the overseas jurisdiction.

Governance

ARIE's AML/CTF Compliance program, policy and procedures are reviewed and approved by the senior management.

ARIE has an independent Risk & Compliance Department responsible for the Compliance functions of the organization. The Head, Risk & Compliance is the authorized Money Laundering Reporting Officer (MLRO) of the company.

The Department comprises of Senior Risk & Compliance Officers, Risk & Compliance Officers, and branch level Compliance Monitoring Officers (CMO).

All day to day functions and monitoring of the AML/CTF related activities are handled by the Risk & Compliance Department. A daily reporting system is established for routine reporting, review and escalations as necessary. ARIE has an AML/CTF Committee which comprises the key officials of the organization and is headed by the General Manager (Chairman of the

committee). The other members to this committee and the responsibilities are mentioned in the table below.

Structure	Responsibilities
Head of the committee - General Manager Members - • Head - Risk & Compliance • AGM – Operations • Sr. Manager – Finance & Admin. • Manager – Quality & Business Excellence • Area Managers – Branch operations • Compliance officers	• To review the current challenges / issues and to ensure proper controls are in place. • To take corrective / preventive actions if any gaps are identified. • To discuss the current trend and requirements of the Regulators / Authorities To discuss the following areas and actions if any needs to be taken. ✓ Updates on sanctions ✓ Notices / Circulars received from regulatory authority ✓ STRs raised during the month ✓ ECDD conducted during the month ✓ Trainings conducted / attended ✓ Feedback / Queries received from regulatory authority / correspondent banks. ✓ Pattern Analysis conducted during the month ✓ New product / process risks associated with AML.

The AML Committee shall conduct Quarterly Meetings to discuss AML/CTF matters, review Action Plans and recommended follow up actions based on outcomes of review, The Committee shall also discuss initiatives required to be undertaken to continually improve ARIE's accomplishment in the areas of AML/CTF.

Money Laundering – An Overview

Money Laundering is a process whereby criminals attempt to hide the true origin and ownership of the proceeds of their criminal activities thereby avoiding prosecution, conviction and confiscation of the criminal funds. Money Laundering involves in 3 stages;

1. **Placement**- the stage at which criminally derived funds is introduced in the financial system.

2. **Layering**- Separating the proceeds of criminal activity from their origins through layers of complex financial transactions.
3. **Integration**- the final stage at which the 'laundered' money is re-introduced into the legitimate economy.

The fight against money laundering is an evolving and never ending process. Money laundering not only harms the public as a whole, but it shakes the financial services industry. It is clearly in the best interest of the financial industry to take appropriate actions to prevent money laundering.

Terrorist Financing

Terrorist financing refers to the processing of funds to sponsor or facilitate terrorist activity. It may involve funds raised from legitimate sources such as personal donations, profits from the businesses and charitable organizations as well as from criminal sources, such as the drug trade, the smuggling of weapons and other goods, fraud, kidnapping and extortion.

This is one of the major threats faced by all financial institutions globally. ARIE aims to prevent from being used for funding terrorist activities and shall be alert always to report suspicious transactions if any.

Know Your Customer and/or Know Your Customer Counter Party" (KYC/KYCC) Policy

KYC and KYCC are effective defenses against laundering money and/or terrorist financing. ARIE Systems are designed to capture all the relevant information of the customer and the beneficiary prior to processing a transaction. The controls built in the System ensure that customer and beneficiary information is mandatory to obtain while processing a transaction.

This is a vital preventive approach that supports in effectively filtering suspicious activity in a proactive manner, and in compliance with regulatory requirements.

ARIE ensures that the key information and documents to support effective KYC and KYCC include:

a) Complete name of Remitter or Remitting Company as per the identity card/Trade License Name)
b) Complete address
c) Contact number
d) ID details (Type of ID & Date of issue & expiry date)
e) Job profile/line of business
f) Source of funds
g) Purpose of transaction
h) Relationship with the beneficiary
i) Ultimate Beneficial Owner (UBO)
j) Copy of valid ID
k) ARIE staff shall always sight the original ID from the Remitter, and initial a copy of the ID as "True Copy".

In rare events or incidences where a Customer fails to provide adequate KYC information, or appears hesitant/unwilling to provide information as required to establish adherence to KYC norms, ARIE shall not proceed with a transaction for such as Customer, and flag the case as a High Risk customer. Such cases are marked for reporting to the Regulator through Suspicious Transaction Report (STR), and for increased monitoring.

Customer onboarding

ARIE's customer onboarding process utilizes System capabilities supported by sound personal experience and knowledge. In general, ARIE has 3 categories of customers;

1. Retail/individual customer
2. Corporate/SME customer (CFE/SME)
3. Wholesale customer(WC)

Retail customer onboarding is performed by the branches where Customer data is entered into the System. The data/name entered is screened against the watch list automatically, on a real time basis. In case of any name match, the System alerts the Branch User and prohibits processing of the transaction without a clearance from the Compliance Department. Such clearance is generally provided only after conducting enhanced screening using "World Check" and web search.

Furthermore, at the transactional level both the remitter and beneficiary names will be once again screened against the watch list. In case of any match, the transaction will be on hold under "suspicious transaction" dash board for the compliance clearance. False positive case will be released to go ahead and exact match case will be rejected and/or reported to Central Bank through STR.

As per the internal policy all corporate customer onboarding shall be done only after Compliance clearance. The branch staff shall obtain all mandatory documents and provide the same (listed below) to the Compliance department.

1. Completed CFE application form – Signed by the customer.
2. Valid copy of trade/commercial license
3. Memorandum/Articles of Association (MOA/AOA)- whichever is applicable
4. Valid passport copies of owner, partner(s), authorized personnel and POA holder(s).
5. Partnership deep – If applicable
6. Copy of Power of Attorney (POA)
7. Site Visit Report (SVR)
8. Authorization letter from the customer

Customer onboarding policy is applicable to Wholesale currency buy/sell customers as mentioned below;

1) Retail/Individual – Similar to a Retail Customer onboarding, where KYC check and automated name screening is enabled through the System.
2) Corporate customer- Corporate onboarding policy applicable (as mentioned above)

3) Exchange houses- Copy of valid trade license, Passport copies of owner and/or partners and completed AML/CTF KYC questionnaire required.

Compliance clearance request received from the branches shall be scrutinized by the Compliance officer to ensure its completeness. The compliance officer shall perform "World-check" and "web search" to find out any negative news/remarks. Based on the outcome, the feedback with the remarks will be sent to the branch either to "accept or reject" the customer. False positive case will be released to go ahead and exact match case will be rejected and/or reported to Central Bank through STR.

Due Diligence (DD)

ARIE shall do due diligence before on boarding the customer or establishing business relationship with the correspondent banks, service providers and business partners.

Enhanced Customer Due Diligence (ECDD)

ARIE shall perform Enhanced Due Diligence in the following scenarios;

1. Before onboarding the customers dealing with;
    a) Jewelry and precious stones
    b) Real Estate
    c) Luxury items
    d) Auction houses
    e) Non-resident account holders/visitors
2. The customers of high risk countries/products/services etc.
3. Politically Exposed Persons (PEPs)
4. If the customer/transaction found to be suspicious/unusual.
5. Any other suspicious cases alerted by the system based on the rule violation(s).

The above scenarios are reviewed periodically and updated as required through the quarterly Compliance Committee Meeting.

Transaction Monitoring

ARIE is committed to fight against money laundering and/or terrorist financing hence the AML/CTF compliance program includes well established policies, procedures and an automated transaction monitoring system which is called "Omni AML Solution" powered by Infrasoft Technologies. The AML solution is integrated with the core application (iCARE) and it has customized online and offline rules and parameters to pick up the rule/threshold violation(s). Once rule violations are picked up by the system then it will further undergo review and analysis by different hierarchies of Compliance Officers. The outcome/action taken includes clearing of 'false positives' or 'creation of case' for STR.

ARIE's AML solution has the capability to store the watch lists such as OFAC, UN, EU, HM and the list of names issued by Central Bank and Law enforcement. Additionally, to support and comply with demand from competent Authorities as required, the System has the capability to maintain an internal black list to "add" or "remove" the names as communicated by the

Authorities. This function is handled by the Risk & Compliance Officers who have limited access to create the internal Black List.

The lists are updated on daily basis if there are notices/alerts from regulatory authorities for the purpose of screening the names to identify the prohibited individuals, entities, organizations who may pose a high risk to the global community/financial systems.

Reporting of Suspicious Transaction Report (STR)

ARIE shall file suspicious transaction report to Central Bank, if there are reasonable grounds to suspect that the proceeds are from the outcome of any of the illegal activities and/or the transaction is intended for terrorist financing/activities. If any such incidents are detected Risk & Compliance Department is responsible to file STR with Central Bank using the online portal. However, it is the responsibility of all ARIE staff to identify and notify suspicious/unusual transactions to the Risk & Compliance Department.

The process to be followed in filing STR is initiated at the Front end, where staff is empowered to manually flag a transaction as 'suspicious' by marking the same in the Core Application or raising it through e-mail or phone correspondence with the Compliance Officer on duty.

The suspicious notification received from the branch/es to be reviewed by the Compliance officer and to submit the findings/valid grounds of suspicion to the Head of Risk & Compliance for further review, validation and approval.

Once approved by the Head of Risk & Compliance, the STR is filed through a direct upload into the Central Bank online portal along with the necessary supporting documents and using the four eye concept ("maker" and "checker").

The outcome of the STR shall be shared with the senior management of ARIE if the response demands to do so.

The STRs filed are discussed in the AML Quarterly Committee Meeting.

Tipping off

ARIE policy governs that staff of ARIE shall not warn or share the information with the concerned individual and/or entity about the information being reported to/investigated by the relevant authority. Any deviation to these guidelines shall attract disciplinary action. All staff shall be made aware of this responsibility

On-going KYC/Periodic review

ARIE shall conduct periodic review and update the KYC information of all its customers on on-going basis. However for high and medium risk customers' frequent review will be done based on the transaction trend, nature of business and event driven scenarios such as expiry of trade license or Identities, change in office location, trading name, management, correspondent bank query, notice from Central Bank or Law Enforcement,

Record Retention

ARIE shall retain all its customer/transaction related data/supporting documents for a period of 10 years from the date of closure of business/date of transaction.

Prohibited Business/Relationships

ARIE shall not enter into a business relationship with any of the shell company/bank/service provider. For the existing customers, during the course of business relationship if there are reasonable grounds to believe that the client/service provider involve into any of the illegal activities, relationship with such clients / service providers will be suspended/terminated with immediate effect and will be reported to the regulatory authority.

Sanction Policy

ARIE shall not conduct any transaction to/from any sanction country and will not undertake/accept any transaction to/for individual, entity and/or country name which are black listed by the local and/or any of the international regulatory authorities.

PEP Transactions

Financial transactions of Politically Exposed Person generally possess high risk due to the potential involvement in bribery and/or corruption. Hence, onboarding of PEP customer requires compliance clearance and senior management approval. At the transactional stage, it requires proper satisfactory supporting documents to substantiate the transaction. Failure to comply the supporting documents by the customer shall be reported to the regulator.

Correspondent Banking Relationship

ARIE shall enter into a correspondent banking relationship only after considering the following factors and with the approval of the Management;

1) After conducting proper KYC/Due Diligence.
2) Ensuring that the Correspondent Bank has a documented AML/CTF policies and procedures.
3) Ensuring that the Correspondent Bank is registered and monitored by a regulatory authority.
4) Ensuring that the Correspondent Bank had not been fined for AML/CTF/ any other major non-compliance.
5) Ensuring that the Correspondent Bank has a physical existence in their home country.
6) In addition to the above, ARIE will also obtain an approval from the Central Bank of the UAE before commencement of relationship with them.

Anti-Bribery and Corruption (ABC) and Anti- Fraud

ARIE will not tolerate any form of bribery, corruption and/or fraud. All ARIE employees are strictly prohibited from having any involvement in the act of such activities. Any non-compliance to this act shall attract disciplinary action.

Staff Reliability

ARIE has process in place in co-ordination with Human Resource Department to ensure that only reliable staffs are employed to the organization.

Training program

ARIE has a comprehensive AML/CTF training program to ensure that all staff, specifically staff involved in the customer onboarding, transaction processing and maintaining customer relationship undergoes AML/CTF training without fail. AML/CTF training is organized by the Quality and Business Excellence Department and handled by Risk & Compliance Department.

As per ARIE's best practice AML/CTF training is a constant education/ awareness process wherein the staff are selected with a combination from frontline, relationship and back office. The existing staffs will be called for a refresher 'workshop' minimum once in every year covering the entire staff. The new joiners will have to attend the induction training within 3 months from the date of joining. However while joining the organization, the branch manager to give a briefing to the new employee about the basic KYC check and AML/CTF Dos and Don'ts. Additionally, during monthly branch meeting the staffs are to be briefed on important AML/CTF updates.

As part of this program, ARIE conducts series of tests and exams covering AML/CFT areas. During training pre and post evaluation tests are conducted to ensure its effectiveness. As a new initiative, ARIE has implemented an AML/CTF self-learning module which is an online platform wherein the staff will have the option to access the URL and refer the AML/CTF related scenarios, incidents and to answer the questions through online.

Business/ Product Risk Assessment

ARIE shall introduce a new product/process only after ensuring that the new product/process has the capability to arrest possible AML/CTF risks. The current products are as follows;

1. Remittance
    a. Direct Credit
    b. Bank to bank
    c. Instant Credit
    d. Pay on ID
2. Demand Draft
3. Encashment of Travelers cheque
4. Buying and selling of currencies
5. Instant money
    a. Send
    b. Receive
6. Ancillary products;
    a. National bond sale
    b. Cash Passport Card (Multi Currency Prepaid Card)
    c. Ezetop mobile top ups
    d. Credit card bill payment

e. Cash advance against credit card
f. Issuance of Air tickets (Air Arabia & Fly Dubai)

Customer profiling or risk assessment

Risk rating scale is used to categorize or classify the customers based on predetermined parameters and AML rules. KYC risk rating is conducted based on the customer profile or nature of business, geography, and nationality. Transactional risk rating is conducted based on the transactional behavior/trend/pattern, nature of product/process/channel type the customer use through the financial institution and the number of violations against the set AML rule(s).

Risk rating scale

Risk Category		
Sr. No.	**Total AML Risk Rating Score**	**Risk Category**
1	<4	Low Risk
2	<6	Medium Risk
3	6 to 10	High Risk

Risk Rating Weightage

Total AML Risk Rating		
Sr. No.	Parameter	Weightage
1	Business intelligence Risk	50%
2	Transaction Type Risk	15%
3	Transaction Trend Risk	20%
4	Rule Violations Risk	15%
	Final AML Rating	100%

Risk Based Approach

The Risk based Approach is a key element for our effective implementation of AML/CTF policies and processes. The Senior Management has introduced the application of Risk Based approach in the following scenarios;

1. Onboarding the customer
2. Rejecting the customers
3. Accepting transactions
4. Accepting supporting documents
5. Accepting high value cash transactions

Any other relevant factor which needs to be considered under this category.

Audit/Independent Testing

The effectiveness to the AML/CTF Compliance program is subject to independent testing of Internal and external audit function.

ARIE has its internal auditors who test/check the AML/CTF effectiveness across the branches and head office on frequent basis. The test results or audit feedback will be shared with the operations team for improvement or corrective action if any. In addition to this, periodically ARIE deploy external audit firms to independently check the effectiveness of AML/CTF compliance.

Wolfsberg /Self-attested KYC/AML/CTF Questionnaire

ARIE has a self-attested KYC/AML/CTF questionnaire drafted in line with the Wolfsberg KYC principle, regulatory requirements of the UAE and other international regulatory bodies. These questionnaires are subject to frequent reviews and modifications to accommodate the regulatory and/or industry changes.

Procedure review and updation

ARIE constantly review the AML/CTF policies/procedures to accommodate the regulatory and/or industry changes. This responsibility lies with the Risk &Compliance Department and any changes are subject to the Committee approval.

Terms and definitions

Customer Due Diligence (CDD)

Customer Due Diligence refers taking steps to identify the customer and their back ground. This includes the process of obtaining full name, complete address, contact number, verifying an official/legal identity card on which the customers photograph is placed, line of business/job profile, source of funds, relationship between the underlying parties etc. In general, it is the act of exercising reasonable care before entering in to business relationship. Additionally, the financial institution should collect the information for what purpose the relationship is established (E.g. remittance, forex/whole sale, wage payment service etc.). Due diligence is one of the way of preventing illicit funds transfer through the financial systems.

Enhanced Customer Due Diligence (ECDD)

Enhanced Customer Due Diligence is an extra measure applied besides the usual Customer Due Diligence to know more about the customer and his/her transactions and his/her physical

business to confirm that purpose & source of funds are legitimate and matches the profile of the customer. ECDD is applicable where the customer's nature of business and their nature of payment request/transaction combination is considered to be high risk or if there is valid reason(s) to suspect the customer/transaction. This activity consists of gathering of additional information which includes but not limited to;

- The customers local and overseas clients
- Countries and parties involved in the transaction
- Nature of business and frequency/volume of transaction
- Ultimate beneficiary destination/nationality
- Business relationship between the remitter and receiver
- Review of documents related to the transaction such as invoice/bill of lading, bank statements/source of funds documents, site visit report etc.

Risk Based Approach (RBA)

Risk Based Approach is a process which enables the financial institution to identify potential risks and to take remedial actions to prevent such vulnerabilities. Channelization of illicit funds and terrorist financing is one of the major threats faced by the financial institutions. Applying RBA approach will help the financial institutions to be proactive in averting such harmful activities.

Transaction Monitoring

Pattern analysis is an offline tool used to evaluate the transaction behavior of the customer based on the transaction history compared with the nature of business/job profile. This process is based on certain criteria such as nature of business, nature of payment request/payment order, number/frequency of transaction, volume, currencies, remitter and beneficiary relationship, mode of payment and availability of supporting documents etc. Pattern analysis helps the financial institutions to determine the level of risk exposed by their customers.

Black list/Watch list screening

A scientifically well-defined watch list screening is an inevitable component of AML/CTF compliance program to detect and prevent money laundering and/or terrorist financing. For this purpose, financial intuitions are using number of screening lists internally prepared by the Financial Institutions, lists issued by the local as well as international regulatory authorities such as notices/circulars from Central Bank of the UAE, Law enforcement, Office of the Foreign Assets Control (OFAC), European Union (EU), United Nations (UN) and Her Majesty (HM).

Suspicious Transaction Reporting (STR)

All financial institutions are required by Law, to file suspicious transaction report to the Financial Intelligent Unit (FIU) of that particular country and this obligation is applicable to the entire employees of the organization. Since ARIE operations are based in United Arab Emirates, any suspicious and/or unusual transaction/customer to be reported to the FIU of Central Bank of UAE viz AMLSCU (Anti-Money Laundering and Suspicious Case Unit

Customer profiling/ Risk Assessment

A scientific method applied to identify the potential risk or vulnerabilities to an organization from its customers. Risk Rating or customer profiling is an ongoing process initially it starts while on boarding the customer which is called as KYC risk rating or profiling. During the course of relationship based on transactional behavior or pattern the profile undergoes further reviews and analysis which results for transactional risk rating.

Shell Company

Shell Company is a company which serves as a vehicle for business transactions without itself having any significant office/assets/operations. Some shell companies may have had operations, but those may have shrunk due to unfavorable market conditions or company mismanagement. A shell corporation may also arise when a company's operations have been wound up, for example following a takeover, but the “shell” of the original company continues to exist. Certain shell companies do have legitimate business purposes, but are used for tax avoidance.

Politically Exposed Customer (PEP)

Politically exposed person (PEP) is a term describing someone who has been entrusted with a prominent public function, or a relative or known associate of that person. PEP generally presents a higher risk for potential involvement in bribery and corruption by virtue of their position and the influence that they may hold.

Money Laundering Reporting Officer (MLRO)

An official of a financial organization who is responsible for monitoring and reporting suspicions related to money laundering and/or terrorist financing. Employees of the organization must report such suspicions to the MLRO.

World-check

World-check is a part of Thomson Reuters risk management solution, world-check data base of Politically Exposed persons and heightened risk individuals/organizations is used around the world to help to identify and manage the financial, regulatory and reputational risk. World-Check’s intelligence is used by banks and financial institutions as a comprehensive solution for assessing, managing and remediating risk.

-End of Policy-

Note: A detailed AML/CTF Compliance procedure is annexed [BOP-(22)] which serves as a ready reckoner for all ARIE employees for their understanding and adherence.

******