Policy

Anti-Money Laundering and Counter Terrorist Financing

A Lulu Exchange Policy document

Document #

POL-AE COMP001

Created

Updated

12/03/2018

Controller

Compliance Officer

Owner

Chief Compliance Officer

Confidentiality Statement as per its classification below, and the rules of disclosure.

All documents within Lulu Exchange are classified in the following way. **PUBLIC** documents are intended for anyone, **COMPANY CONFIDENTIAL** documents are to be kept confidential within Lulu Exchange, and used for normal business activities by the general office population, **HIGHLY CONFIDENTIAL** documents are to be kept confidential to restricted individuals within Lulu Exchange.

Classification **Company Confidential**

LuLu International Exchange لولو العالمية للصرافة

Revision History

Date	Version	Author	Comments (including Review History)
07/2017	V 3.0	Derick Vincent Saldanha	Updated from the previous version
12/08/2017	V 3.0	Christos Christou	Corrections and spelling check; finalised version
12/03/2018	V 4.0	Christos Christou	Updated to reflect the STANDARDS issued by the CBUAE on 01 March 2018 (Notice No. 35/2018)

Contents

1 Summary

Purpose	The purpose of this Policy is to describe the fundamental principles that all members of Lulu International Exchange L.L.C. must fully comply with, regarding Anti-Money Laundering (AML) legal and regulatory framework and the legal and regulatory framework of Combating the Financing of Terrorism (CFT)., based on the Notice No. 35/2018 – the STANDARDS issued by CBUAE.
Scope	The Policy applies to Lulu International Exchange L.L.C. ("Company"), its associates, branches, or affiliates that provide financial services to customers, as described in the applicable law(s), regulations, or directives of the respective country the entity is operating in, relating to the prevention of the use of the financial system for the purpose of money laundering and financing of terrorism.
Functional Responsibility	The functional responsibility of this Policy lies with the Compliance Officer

2 Related documents

Policies	POL-AE Sanctions Policy
Procedures	PRD-AE AML/CFT Procedures
Work Instructions	WI-Compliance Investigations
Forms	
Other	

3 Definitions

Term/Acronym	Description
AML	Anti-Money Laundering
BoD	Board of Directors
CBUAE	Central Bank of the UAE
CDD	Customer Due Diligence – the process where additional information about a customer, who is a natural person, is collected via a customer onboarding process.
CCO	Chief Compliance Officer/Money Laundering Reporting Officer
CO	Alternative Compliance Officer
Company	Lulu International Exchange L.L.C., its branches, associates, and affiliates
CFT	Combating the Finance of Terrorism
EDD	Enhanced Due Diligence – it is the method of collecting additional evidences and answers about a customer and or a transactions during an investigation procedure.
FID	Financial Intelligence Department
KYC	Know Your Customer - it is the process that the financial services providers and other regulated entities must perform in order to identify their customers (existing or prospecting), collect and record relevant information, static and professional/business related data.
ML	Money Laundering - it is the direct or indirect participation in any transaction that seeks to conceal or disguise the nature or origin of funds derived from illegal activities.
Money Laundering Risk	it refers to the risk of been engaged directly or indirectly with money laundering, terrorist financing, or proliferation.
Proliferation	It is the act of production, distribution, or usage of arms or armaments of mass distruction.
Risk-based approach	a reasonably designed risk-based approach is one by which institutions identify the criteria to measure the potential money laundering risks.
STANDARDS	The Standards for the Regulations Regarding Licensing and Monitoring of Exchange Business – Notice No. 35/2018

STR	Suspicious Transactions Report filed with FID; however, the term **iSTR** can be also used to mean "internal" Suspicious Transactions Report and is filed within the Company by employees independently directly to the Compliance Officer
TF	Terrorist Financing - it is the act of providing any material, or facilities, or collection of financing, or managing of funds aiming to perform, facilitate, or assist the commission of a terrorist act by a criminal organization or individual terrorist.

4 Introduction

The Company is operating under license from the CBUAE to offer the financial services products of "foreign currency exchange", "remittance operations", "payment of wages using WPS", and "special products or services"; in this respect, it is under legal and regulatory obligation to design and implement a formal and effective AML/CFT Compliance and Sanctions Program based on Paragraphs 16.2 to 16.30 of Chapter 16 of the STANDARDS, as a minimum.

The Company has implemented additional AML/CFT procedures, systems, controls, and measures appropriate to its risk profile.

The Company's Board of Directors has nominated and appointed a Compliance Officer, who has been approved by the CBUAE, to direct and manage the AML/CFT Compliance and Sanctions Program, supported by an Alternative Compliance Officer (D-MLRO).

The Board of Directors has also approved a number of other compliance policies, including the POL-AE Sanctions Policy, that must be strictly followed by all the members of staff of the Company.

5 AML/CFT Policy Statement

The main objectives of the Company's AML/CFT Policy are:

- To comply with the provisions of Federal Law No.9 of 2014;
- To abide by the STANDARDS issued by the CBUAE (Notice No. 35/2018) and to assist the authorities in combating Money Laundering and Terrorist financing;
- To abide by the FATF recommendations;
- To abide by the Wolfsberg Group recommendations;
- To ensure that company and its staff will not knowingly assist anyone to launder the proceeds of any act prohibited by the UAE Legal and Regulatory environment and defined as predicative offences;
- To comply with all the primary sanctions regimes and implement automated systems to check and validate any transaction that may be related directly or indirectly to a sanctioned individual or entity.

6 Policy Notes

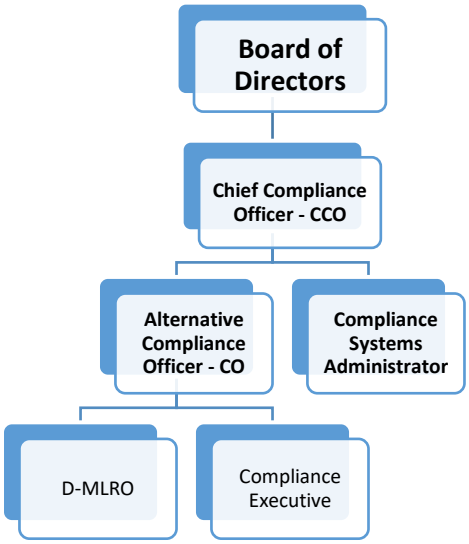
6.1 Organizational Structure

The Board of Directors of the Company has appointed a Chief Compliance Officer to direct and manage the Compliance Function within the Group; based on this, the compliance department has the following structure:

- **Chief Compliance Officer** – heading the Compliance Department and directs the compliance function; the CCO reports directly to the Board of Directors; the CCO is the nominated and approved by the FID as the "**Compliance Officer"**;
- **The Compliance Officer** – responsible to manage the compliance function; the CO reports directly to CCO; he is approved as the "**Alternative Compliance Officer**" by the FID;
- **The Deputy Compliance Officer (D-MLRO)** – responsible for investigating and reporting any suspicious transactions to the CO and or CCO;
- **The Compliance Executive** – is responsible to support the compliance investigation process within the Compliance Team, and reports to the CO and or CCO.

Special Note: The Company has initiated an internal procedure, and appointed the Branch Managers as Branch Compliance Officers (BCOs), as an additional control measure; they are responsible for implementing the AML/CFT policies and procedures within their branch and report any suspicions directly to the Compliance Officer through the formal iSTR procedure/form.

FUNCTIONAL ORGANIZATIONAL CHART OF COMPLIANCE DEPARTMENT



6.2 Responsibilities for the AML/CFT Compliance Function

- **Board of Directors**:

Based on Chapter 6, Paragraph 6.7 of the STANDARDS the Company must appoint a BoDwith the following roles and responsibilities:

- To oversight all activities of the Company;
- To appoint and monitor the performance of the Manager in Charge;
- To maintain honesty, integrity, and transparency throughout the business activities;
- To ensure a robust and independent compliance function is established and maintained;
- To ensure the appropriate AML/CFT Compliance and Sanctions Program and other related Policies are implemented;
- Ensure that actions are taken by the relevant stakeholders to resolve internal/external audit findings and regulatory compliance issues including AML compliance in a timely manner;
- Ensure that sufficient time, freedom, resources, systems, and tools are available for the Manager in Charge and Compliance Officer to fulfil their responsibilities effectively;
- Ensure that an internal function is established and maintained;
- Review the effectiveness of the internal audit function at the end of every year.

- **Chief Compliance Officer**:

The Company must appoint a Compliance Officer who must be given the specific responsibility by the BoD of managing its AML/CFT compliance function. The Bod of the Company has appointed the Chief Compliance Officer who has the following role and responsibilities:

- Design an appropriate AML/CFT Compliance and Sanctions Program for the Company to remain compliant with applicable AML/CFT Laws, Regulations, Notices, the STANDARDS, and international best practices at all times;
- Establish and maintain appropriate AML/CFT policies, procedures, processes and controls;
- Ensure day-to-day compliance of the business against internal AML/CFT policies and procedures;
- Act as the key contact point regarding AML/CFT related matters/queries from the CBUAE and any other competent authorities;
- Receive suspicious transaction alerts from employees and analyze them to take appropriate decisions to report all suspicious cases to the FID;
- On-going monitoring of transactions to identify high-risk, unusual and suspicious customers and transactions;
- Submit STRs to the FID in a timely manner;
- Cooperate with and provide the FID with all the information it requires for fulfilling their obligations;

- Develop and execute AML/CFT training programs considering all relevant risks of ML/TF and financing illicit organizations including the way/means for addressing them;
- Provide necessary reports to the BoD on all AML/CFT issues, on a quarterly basis at a minimum;
- Arrange to retain all necessary supporting documents for transactions, KYC, monitoring, STR and AML training for the minimum period of record retention;
- Conduct regular gap analysis between the Company's existing AML/CFT Policy and Procedures and current Law, Regulations, Notices and STANDARDS in order to determine the extent of the Company's level of Compliance;
- Propose actions required to address gaps, if any;
- Prepare Bi-Annual Compliance Reports (see appropriate section in this Policy).

- **Alternative Compliance Officer**:

The Company has appointed an Alternative Compliance Officer in order to strengthen its compliance function. The Alternative Compliance Officer has the same role and responsibilities as the Chief Compliance Officer, as is providing assistance at all times; however, in case of absence of the Chief Compliance Officer, the Alternative Compliance Officer is fully responsible for the Compliance Function, and has the authority to act without the interference from the Manager in Charge.

The Alternative Compliance Officer is directly reporting to the Chief Compliance Officer, and directly to the BoD in case of absence of the Chief Compliance Officer.

- **D-MLRO:**

The D-MLRO is a member in the Compliance Team that is primarily responsible to assist the Chief Compliance Officer, or the Alternative Compliance Officer in his duties; more importantly, the D-MLRO's role is:

- Assist the CO in identifying, documenting and assessing the compliance risks associated with the Company's business activities related to AML/CFT;
- Assist the CO in developing new practices and methodologies for the measurement of compliance risk;
- Assist the CO in identifying, with the assistance of compliance consultants or external legal advisors, the AML/CFT regulatory framework which governs and or affects the operations of the Company, including the creation and maintenance of an up to date register of the existing regulatory framework including evaluation of compliance;
- Assist the CO in creation of Country compliance procedures, if required ensuring alignment with the Company's Compliance Policies;
- Assist the CO in maintaining effective communication with the local regulatory authorities. Developing, documenting, implementing and executing a regulatory compliance program, including AML/CFT;

- Assist the CO in analyzing the Internal Suspicious Transactions Reports (iSTRs), and takes any measure to manage these in the most appropriate manner, so as to avoid any risks imposed on the Company;
- Assist the CO in conducting ongoing monitoring of the country's' operations and activities and evaluating associated AML/CFT compliance risks;
- Assist the CO in communicating new guidelines/instructions issued by Regulators to various departments of the Company, thereby ensuring compliance with the guidelines/instructions issued;
- Assist the CO in making sure that the Organizations' AML/CFT Compliance Policies and Procedures are updated with the latest Legal and Regulatory requirements of the country, in line with the Organization Policies, and are approved by the Board of Directors;
- Assist the CO in ensuring that all employees within the company are trained annually (or more frequently according to the Legal and Regulatory Requirements of the country) on AML/CFT, with special attention on the country AML/CFT Regulatory Framework and on the latest AML/CFT Policy & Procedures;
- Investigate all assigned alerts from the AML System, or reports from YOM System, for identifying possible suspicious transactions;
- With the approval of the CO, inform the FIU formally for any suspicious transactions;
- Substitute the CO and execute the CO's role if the appointed CO is not in the office.

- **Compliance Executive**:

  - Investigate all assigned alerts from the AML System, or reports from YOM System, for identifying possible suspicious transactions;
  - Investigate all ad-hoc requests from any competent authority;
  - Support the CO in any type of compliance investigation requested.

6.3 Know Your Customer (KYC) Policy

The Company has approved and is implementing a risk-based approach in applying appropriate customer due diligence, based on the identified AML/CFT risks associated with each customer, but moreover to confirm who their customers are and that the funds used for the transactions come from legitimate sources and used for legitimate purposes.

In general, the Company has set the following minimum policy related to know-your-customer:

6.3.1 Customer Identification Process

6.3.1.1 Individuals

- Customer identification, i.e. presentation of the valid identification document described below, is mandatory for all individuals that want to execute a **remittance transaction (inward or outward) for any amount**;
- Customer identification, i.e. presentation of the valid identification document described below, is mandatory for all individuals that want to execute a **foreign currency exchange of an amount more than AED3,600 per transaction**;
- Customer identification, i.e. presentation of the valid identification document described below, is mandatory for all individuals that want to execute a **foreign currency exchange of an aggregated amount more than AED3,600 per week**.

The type of identification documents that are acceptable during the customer identification process are:

Residents

a. Valid Emirates ID
b. Valid UAE National ID
c. Diplomatic ID – **only for members of the embassies and international organizations in UAE**

Non-residents

a. Valid Passport with valid entry visa
b. Valid GCC National ID (for GCC nationals)
c. Seaman's Pass/ID

The original identification document must be collected at all times during the Customer Identification Process, a photocopy should be produced by the FLA in the Branch, and it must be stamped as "Original Verified" and signed by the FLA; the certified copy must be maintained at all times in our records as per the SOPs.

6.3.1.2 Corporates

- Customer identification process for corporates is followed irrespective of type and amount of any transactions executed;
- Customer identification process for corporates is followed independently and during the customer registration procedure.
- **NO customer registration is allowed for corporates that have been registered, or have their registered, office outside the UAE.**

The type of identification documents that are acceptable during the customer identification process are:

a. Commercial License, from a government office or responsible ministry, e.g. Chamber of Commerce and Industry, Ministry of Commerce etc.;
b. Trade License from a government office or responsible ministry, if different from the Commercial License;

c. Business License, e.g. Central Bank license, if the corporate is a financial services provider;
d. Identification documents for every shareholder/partner/owner of the corporate;
e. in case any of the shareholder/partner/owner is another corporate, the identification document of the shareholder/partner/owner of that corporate;
f. repeat the steps "d" and "e" until the shareholders/partners/owners of any corporate are individuals – **ultimate beneficial owners**.

6.3.2 Customer Due Diligence

CDD is executed for all individuals that:

a. Execute any **single foreign currency exchange** transaction that is **between AED36,000 and AED99,999**;
b. Execute any **total foreign currency exchange** transaction that is **between AED36,000 and AED99,999 within 90 calendar days**;
c. Execute any **single remittance** transaction that is **between AED1 and AED74,999**

All individuals that want to execute any type of transaction described in the Section 6.3.2 **must be fully registered BEFORE executing the transaction**; the procedure followed for customer registration must include the following data and information are **mandatory** recorded in the System:

- Full legal name, as described in the original Identification Document presented;
- Residential status, i.e. "resident" or "non-resident";
- Full residential address (for UAE residents);
- Temporary residential address for non-UAE residents, e.g. hotel name and room, and permanent residential address outside UAE;
- Mobile number;
- Email address;
- Date of Birth;
- Nationality;
- Country of Birth;
- ID type, and ID number;
- ID place of issue, ID issue and expiry dates;
- Profession;
- Expected annual activity.

For existing, or already registered customers, the FLA must **always collect the original identification document to verify the identity of the individual presented in the counters**.

The customer profile, i.e. the individual customer data and information collected and input in the System must be maintained every year, or after the expiration of the identification document used (whichever comes first), and CDD process is repeated again.

6.3.3 Enhanced Due Diligence

6.3.3.1 Individuals

EDD is executed for all individuals that:

a. Execute any **single foreign currency exchange** transaction that is **above AED100,000**;
b. Execute any **total foreign currency exchange** transaction that is **above AED100,000 within 7 calendar days**;
c. Execute any **single remittance** transaction that is **above AED75,000**.

All individuals that want to execute any type of transaction described in the Section 6.3.3.1 **must be fully registered BEFORE executing the transaction**; the procedure followed for customer registration must include the mandatory data and information recorded in the System, as described in Section 6.3.2.

The EDD **additional evidences** required for every transaction described in Section 6.3.3.1 are:

- Evidences of source of funds, e.g. bank statement, cash withdrawal slip etc.;
- Complete information of the real purpose of transaction, e.g. AML Self-Declaration form;
- Other evidences for the real purpose in case the transaction is related to sale of property, other asset, or the purpose is unknown to us – example valid original contract of sale/purchase, valid original invoice, statement of customer account etc. accordingly.

6.3.3.2 Corporates

EDD is executed for **all corporate's transaction, irrespective of amount, frequency, or type of transaction**.

All corporates that want to execute any type of transaction described in the Section 6.3.3.2 **must be fully registered BEFORE executing the transaction**; the procedure followed for corporate customer registration must include the mandatory documentation, data, and information as described below:

a. Completed fully, and signed appropriately, corporate booklet which includes the full KYC questionnaire;
b. Ownership structure, signed by the Company's owners;
c. The purpose and nature of the business relationship with the Company;
d. Copies of valid business permissions from competent authorities, e.g. certificates of incorporation, trade license, regulatory licenses etc.;
e. Completed corporate visit, and assessment of the nature of business verified and physical presence/premises by the BIC and AM;
f. Original Identification Documents of Ultimate Beneficial Owners, photocopied and stamped duly verified as true copies of the original;

g. Full list of authorized signatories, managers, and representatives of the corporate;
h. Completed annual activity with the Company, and the expected purposes of the transactions;

The details that must be recorded in the System include:

- Full legal name, as in the certificate of incorporation;
- Residential status;
- Full registered physical address – P.O. Box does NOT suffice as valid registered address;
- Company official phone numbers;
- Fax number details;
- Email addresses of Company officials (where present);
- Date of establishment;
- ID type, and trade license number;
- Trade license place of issue, date of issue, and expiry date;
- Type of business (activity code);
- Expected annual activity with the Company – number and total amount of transactions;
- Connect ALL ultimate beneficial owners, managers, and representatives which **were individually registered with full CDD as stated in Section 6.3.2**

All registrations to be executed to corporates **must be pre-approved by the General Manager and then forwarded to the Compliance Officer for final approval in the System.**

6.4 Customer Acceptance Policy

Customer Acceptance Policy lays down the criteria for acceptance of customers.

- Lulu International Exchange LLC has a customer acceptance policy and relevant procedures in implementation of the regulatory framework in force and of the best practices, so as to avoid relationship with customers against whom sanctions are applied or those who are facing charges for criminal activity or those who may use Lulu International Exchange LLC services for "money laundering" or other criminal activity.
- Lulu International Exchange shall conduct due diligence of any person applying to do business with it. The staff shall obtain satisfactory evidence of the identity and legal existence of persons conducting transactions on the basis of reliable documents or other resources, and record that identity and other relevant information regarding the customers in their files. If a customer refuse to provide his identity card or passport for verification, the transaction shall be refused.

As per the customer acceptance policy of Lulu International Exchange LLC the staff will follow the below guidelines:

- Physically inspect the original customer's identification document (ID).
- Check whether the customer is the person referred to in the identification document.
- Take reasonable steps to ensure that the customer's identification document is genuine.
- Ensure that the records of existing customers remain updated and relevant.
- Check customer's source of income and wealth according to the customer profile.

The Customer Identification process:

A. Individuals:

- Customers Identity must be established and verified before conducting the transaction. ID of all the transactions above AED2000 or equivalent must be collected and verified. As a best practice, it is advised to collect ids of all the transactions. Customer identity must be verified and established for all suspicious or unusual transactions regardless of the amount.
- EMIRATES ID is compulsory for UAE Resident, and any transaction can be executed only with valid Emirates ID. For Non-Residents, a transaction can be executed only with the valid Passport and valid visa. In exceptional cases wherein if the resident has not yet received his/her Emirates ID, then the Branch can execute the only one transaction with Passport and visa with prior approval from Compliance.

B. Corporates:

- All the corporate entities must be identified with a proper license issued by the appropriate authority, and the owner's id copies must be collected and verified. For Exchange houses in the UAE, valid Central Bank License must be obtained along with other documents.

The Customer Due Diligence (CDD) and Enhanced Due Diligence (EDD) process:

- Ongoing CDD must be conducted on all the customers to update the KYC documents, the personal and professional details provided, to understand the transaction pattern, and to avoid any misuse of the financial system and policies. Updated KYC evidences and additional documents should be collected as and when required.
- Additional source of funds verification documents must be collected for all the high-value transactions, frequent transactions, and for all suspicious transactions. Branch staff should collect additional supporting documents wherever applicable. Any suspicion the branch staff has must be sent to compliance, through Internal STR (iSTR) for further investigations and EDD.

6.5 PEP Client Acceptance Policy

PEP

Politically Exposed Persons are those who have been entrusted with prominent public function in a country or territory, or any of their family or closely related partners. The prominent public functions may in this regard include Heads of States, Heads of Government, Ministers, Dy. /Asst. Ministers,

Senior Functionaries of Political parties, Members of Central Banks, Ambassadors, High Profile officers in Armed Forces, CEOs of State Undertakings and many more.

All business relationship with PEPs will be executed normally, as these individuals are not considered as high-risk customers, based on CBUAE Regulations.

FPEP

Foreign Politically Exposed Persons (FPEPs) are those PEPs who have permanent residential address outside the UAE.
Customer Registration will be established with FPEPs only after getting approval from the CCO. If any existing customer, or the beneficial owner of an existing corporate customer, has subsequently found to be linked to or has become FPEP, then the relationship will be continued only after prior approval from the CCO.
FPEPs will be subject to EDD measures, and discreet inquiries must be made for ascertaining the purpose and ultimate beneficial owner for each and every transaction made by them above USD1,000. In case of any suspicion, then an STR has to be filed with the AMLSCU.

6.6 Reporting of Suspicious Transactions

Transaction Screening and Monitoring:

The Company uses modern technology for on-going transactions monitoring. Rules and scenarios are applied for sanction scrrening of all customers and beneficiaries, single transaction monitoring and risk assessment, and profiling and customer transactional behavior. The alerts generated are verified by the Compliance Team, apply EDD, and take appropriate action in case of suspicion.

iSTR and STR:

An Internal Suspicious Transactions Report (iSTR) is raised by the BCO, or Internal Auditors, to the CO in case of any suspicion. All the iSTR are logged with the relevant supporting documents/evidences of suspicion. All the suspicious cases which are reported through iSTR are reviewed and investigated in depth, and any evidenced suspicion is reported to the AMLSCU.

6.7 Know Your Employee and Employee Training

As part of “Know Your Employee” program, the HR Department checks and verifies the collected documents presentated during the recruitment procedure. The HR Department will collect all the appropriate educational qualification certificates, and or professional certificates, duly certified or attested by an appropriate authority.

For critical, control positions, the BoD will issue a special resolution for appointing them, and the CBUAE approval will be taken.

The HR Department will execute a background check, or contact the referenced persons identified by the employee, so as to verify the correctness of the data and evidences provided. The HR Department must request from the CO to execute an independed background check for every employee, and any information found should be communicated confidentially to the HR Department with the Cos reccommendations.

The Company offers AML/CTF training for all employees. The training is compulsory for new employees (part of the Induction Course) and is followed by a training on Basic Pronciples of AML/CFT and AML/CFT Policy and Procedures. The latter is given to every employee via an eLearning Module (eLeap) every 6 months, or through class-room based training internally or through FERG.

All the BCOs are trained on Advanced AML/CFT every six months.

All the records related to training and employee undertaking are collected and stored.

6.8 Record Keeping

The objective of recordkeeping is to ensure that we can provide necessary information about customers, and to reconstruct individual transactions' details at any given time or as per the request of competent authorities or auditors.

All the receipts, records and documents are retained for a minimum period of seven years. These records can be stored as hard or soft copy, and strict process of document control is applicable.

Strict confidentiality is maintained of all the customer's information, transaction history, and related evidences. All members of staff are trained not to share any details related to customers and their transactions.

6.9 Tipping Off

- Tipping off is prohibited under the provisions of Law (9) of 2014 and AML/CFT Regulations;
- We ensure that our management and employees are aware of, and are sensitive to the data sharing, and consequences of tipping off;
- In case the employee believes or has reasonable grounds to believe that a customer may be tipped off by conducting CDD measures or on-going monitoring, the employee should refer the case to CO/MLRO. The CO/MLRO shall maintain records to demonstrate the grounds for belief that conducting CDD measures or on- going monitoring would have tipped off the customer.

- If an internal STR is send to CO/MLRO, the employee should not disclose this to the customer or any other person;
- The company should ensure that information relating to internal STRs are not disclosed to any person other than the members of Board of Directors of the company without the consent of the CO/MLRO;
- The CO/MLRO should not accord permission or consent to disclosure of information relating to internal STR to any person, unless CO/MLRO is satisfied that such disclosure would not constitute tipping off;
- Any letters, notices, or requests received from CBUAE, or FIU, or Police these should not be disclosed to any person/customer.

6.10 Correspondent Relationship

- The CO/MLRO shall gather sufficient information about the correspondent banks with whom the Company is going to enter relationship with, through a structured questionnaire.
- The CO/MLRO must obtain information about the correspondent banks ownership structure and management.
- The CO/MLRO should pay attention to the quality of supervision by the relevant supervisory authorities before establishing correspondent relationships with foreign Banks.
- The CO/MLRO should establish that the banks have due diligence standards and employ due diligence procedures with respect to transactions carried out through the accounts.
- The Company will not enter correspondent relationship with Shell Banks.
- The CO/MLRO must assess the risk involved in such a relationship, through the completion of the form “Compliance Assessment on Third Party Agreements”, and approve or reject such a relationship based on the risk assessment results.

7 Records

Document	Location	Duration of Record	Responsibility
KYC evidences	Branch/Warehouse	7 years minimum	Branch Manager/Warehouse Manager
Employee documents	HR Manager	7 years	HR Manager