

AML/CFT Policy

A Lulu Exchange Co LLC Policy document

Document #
POL-OM COMP002

Created
01-04-2012

Updated
20/01/2019

Controller
Compliance Officer/MLRO

Owner
Chief Compliance Officer

Confidentiality Statement

Information in this document must be kept confidential as per its classification below, and the rules of disclosure.

All documents within Lulu Exchange Co LLC are classified in the following way. **PUBLIC** documents are intended for anyone, **COMPANY CONFIDENTIAL** documents are to be kept confidential within Lulu Exchange Co LLC 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 Co LLC.

© Copyright Lulu Exchange Co. LLC. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the written permission of Lulu Exchange Co LLC.

Classification

Company Confidential



لولو للصرافة
LuLu Exchange

Revision History

Date	Version	Author	Comments (including Review History)
01/04/2015	V.1	Shalimar Kabeer	Created for Asia Express Exchange co LLC
15/05/2015	V.2	Shalimar Kabeer	Updated for Asia Express Exchange co LLC as part of the Consultancy/Business Management Project
01/01/2017	V.3	Binu Gopinathan	Updated by Asia Express Exchange co LLC as part of the continuous update of the Policies and Procedures
16/07/2017	V.4	Binu Gopinathan	Updated by Asia Express Exchange co LLC as part of the continuous update of the Policies and Procedures
15/01/2018	V.5	Binu Gopinathan	Updated by Asia Express Exchange co LLC as part of the continuous update of the Policies and Procedures
20/02/2019	V.6	Binu Gopinathan	Updated by Lulu Exchange Co LLC (formerly Asia Express Exchange Co LLC) as part of the continuous update of the policies and Procedures

Classification

Company Confidential

POLICY

This document is uncontrolled if printed.

Doc ID POL-OM COMP002

Printed

Controller CO

Created 01/04/2015

Updated 20/02/2019

Owner CCO

Page 2
of 14

Contents

1	Summary	4
2	Related documents	4
3	Definitions	5
4	Introduction	6
5	Policy Statement	6
6	Policy Notes	7
6.1	Organizational Structure	7
6.2	AML/CFT General Principles	9
6.3	KYC	9
6.4	Ultimate Beneficial Owners	10
6.5	Tipping Off	10
6.6	Record Keeping	11
6.7	Know Your Employee	11
6.8	Training	12
6.9	Correspondent Relationship	13
7	Records	13

Classification **Company Confidential**

POLICY

This document is uncontrolled if printed.

Doc ID **POL-OM COMP002**

Printed

Controller **CO**

Created 01/04/2015

Updated 20/02/2019

Owner **CCO**

Page 3
of 14

AML/CFT Policy

1 Summary

Purpose	The purpose of this Policy is to describe the absolutely fundamental principles that all members of Lulu Exchange Co LLC 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).
Scope	The Policy applies to Lulu Exchange Co. LLC. ("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/MLRO

2 Related documents

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

AML/CFT Policy

3 Definitions

Term or Acronym	Description
AML	Anti-Money Laundering
BoD	Board of Directors
CDD	Customer Due Diligence – it is the process of collecting, evidencing, and verifying the customer transactional behavior.
CO/MLRO	Compliance Officer/Money Laundering Reporting Officer
Company	Lulu Exchange Co LLC, 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.
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.
CBO	Central Bank of Oman
Risk-based approach	a reasonably designed risk-based approach is one by which institutions identify the criteria to measure the potential money laundering risks.
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.

AML/CFT Policy

4 Introduction

The Company is operating under license from the CBO as a foreign currency exchange and remittance business; in this respect, it is under legal and regulatory obligation to design and implement a formal and effective AML/CFT Compliance and Sanctions Program. The Company's Board of Directors, has nominated and approved a Compliance Officer/MLRO who is approved by the CBO to direct and manage the AML/CFT Compliance and Sanctions Program.

The Board of Directors has also issued and approved a number of compliance policies, including the AML/CFT Policy, that must be strictly followed by all the members of staff of the Company.

5 Policy Statement

Royal Decree No 34/2002 issued on 27 March 2002, Royal Decree No. 72/2004 issued on 27 December 2004 and Royal Decree 79/2010 issued on 28 June 2010, Royal Decree No. 30/2016 issued on 02nd June 2016 has laid out the following AML & CTF procedures which require all employees to strictly comply with.

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

- ◇ **To protect the reputation of the Company**, by taking all reasonable steps for exercising appropriate CDD in all business functions so as to deter the use of the Company's products and services for ML/FT, and all those persons that are involved in criminal activities, including terrorism and proliferation.
- ◇ **To protect the Company's assets, its management team, and its employees** from unfounded allegations of facilitating ML, TF, and Proliferation.
- ◇ **To avoid criminal and or civil legal proceedings, and regulatory sanctions or penalties** which might result from unwitting involvement in ML, TF, or Proliferation.
- ◇ **To avoid any financial losses from criminal and or civil legal proceedings, and regulatory sanctions or penalties** which might result from unwitting involvement in ML, TF, or Proliferation.

The Company is declaring the following:

- ◇ **Identifies the customer before** establishing a business relationship;
- ◇ **Registers all customers executing any type of remittance transactions** (sender, receiver, beneficiary);
- ◇ **Registers all customers executing foreign currency exchange transactions;**
- ◇ **Builds an economic profile of all corporate customers;**
- ◇ Collects, scans, and store a **verified Identification Document**, only from the categories that the CBO allows to be used in financial transactions;
- ◇ Executes CDD for every transaction executed;
- ◇ Applies an automated **Risk Scoring Model to categorize** its customers for ML/FT risk;
- ◇ Undertakes **EDD for high-risk customers**, or customers that want to execute **high-value transactions;**

AML/CFT Policy

- ◇ Is not accepting business relationship with **not accepted person's categories, or shell companies, or executes transactions on behalf of third parties** that do not have an approved legal right to execute transactions for;
- ◇ Implements controls, through MIS reporting and an automated software, to **identify, investigate, and report any suspicious transactional behavior**;
- ◇ Adopts methodologies for **recognizing suspicious transactions at the front-line business operations**, internally report them to the CO/MLRO, and reporting those, if found suspicious after investigation, to the competent authorities (FIU);
- ◇ Complying with the **applicable sanctions** – UN, EU, OFAC, and the instructions of the CBO related to not-acceptable persons (black listed entities);
- ◇ Adopts methodologies and automated systems to **identify, investigate, log, and execute continuous EDD for PEPs**;
- ◇ Puts in place **appropriate controls**, e.g. audits from Internal or External Auditors, so as to assess the effectiveness and efficiency of the AML/CFT Compliance and Sanctions Program;
- ◇ Provides **ongoing training** to all employees of the Company for AML/CFT.

6 Policy Notes

Organizational Structure

- ◇ The Board of Directors of the Company has appointed a CO/MLRO to direct and manage effectively the AML/CFT Compliance and Sanctions Program within the Company's Operations;
- ◇ The CO/MLRO is directly reporting to the Board of Directors, and for this reason it prepares a Quarterly AML/CFT Compliance Report addressed to the Board, highlighting the key Money Laundering Risks the Company is facing and any appropriate actions taken to mitigate them.

The role of the Board of Directors

- The BoD is the ultimate responsible body for approving and directing the AML/CFT function within the Company;
- The BoD is receiving information and reports from the CO/MLRO, and gives instructions to the MLRO of actions to be taken and directions to consider/work with;
- The BoD approves all the Policies and Procedures related to AML/CFT and oversees the proper adherence to the Laws and Regulations in the country, ensuring that the Company fully comply with these Laws and Regulations.

The role of the CO/MLRO

- Oversight on the implementation of AML policies, procedures, systems and controls, including the risk based approach to ML/FT risks;
- Ensure that appropriate policies, procedures, systems and controls are established, developed and maintained to monitor day-to-day operations for compliance with AML law, regulations, policies, procedures, systems and controls and assess regularly [at a minimum Yearly], review the effectiveness of the same to prevent money laundering and terrorist financing;
- The CO/MLRO should be the key and focal person in implementing the AML strategies;
- Supporting and coordinating the BoD's focus on managing the money laundering and terrorist financing risks in individual business areas;

AML/CFT Policy

- Ensure that wider responsibility for preventing money laundering and terrorist financing is addressed centrally;
- Ensuring the AML monitoring and accountability.

Particular Responsibilities of CO/MLRO & D-MLRO are:

- Receiving, investigating and assessing the internal suspicious transaction reports;
- Filing STRs to FIU, immediately once a suspicion is confirmed or Maximum within two working days after completion of necessary investigation.;
- Acting as focal or central point of contact between FIU, the Regulator(s), and State authorities in relation to AML issues;
- Ensure prompt response to request for information by FIU, Regulator(s), and State authorities in relation to AML issues;
- Receive and act on Central Bank of Oman and international findings about AML issues;
- Monitoring appropriateness and effectiveness of the AML/CFT training programmers;
- Reporting to the BoD on AML and CFT issues;
- Exercising all other functions given to Money Laundering Reporting Officer under AML/CFT Law, regulations or on issues relating to AML/CFT;
- Ensure to keep D-MLRO informed of the significant AML/CFT developments;
- The CO/MLRO must execute his responsibilities honestly, reasonably and independently, particularly while receiving, investigating and assessing internal STRs and deciding whether to make a STR to FIU;
- The D-MLRO will function and act as the CO/MLRO during the absence of the CO/MLRO and during the vacancy of CO/MLRO and rules of responsibilities of CO/MLRO applies to D-MLRO.

Branch Operation's Risk Assessment and Branch Visits

- Establishing a listing of priority risk areas identifying high exposure areas of the branch operations as a means of focusing attention on the most High-Risk areas/branches that need an effective balance of formal and informal practices of risk management.
- MLRO/D-MLRO performs branch visits based on the branch risk category, Minimum monthly one time for High Risk branches and once in a quarter for Medium and low Risk branches.

CO/MLRO reports

The BoD would, on a regular basis, decide what general reports should be given to it by the CO/MLRO, including the periodicity of these reports, in order to discharge its responsibilities under the AML/CFT Law and these regulations. At the minimum, every Quarter CO/MLRO should be given report to the BoD for each fiscal year to enable the BoD to consider it within a specified time frame and assess the overall AML/CFT risks that the Company is facing.

The CO/MLRO Report shall assess the adequacy and effectiveness of the AML policies, procedures, systems and controls in preventing money laundering and financing of terrorism. The minimum requirements of the Quaterly Report that shall be submitted to the BoD for each fiscal year should include the following details, but not limited to:

- The numbers and types of internal STRs made to CO/MLRO;
- The number of these STRs that has been passed on to the FIU and the number of STRs that has not been passed on to the FIU, and reasons thereof;
- The numbers and types of breaches by the AML/CFT Law, regulations or the policies, procedures, systems and controls;
- Areas where the AML policies, procedures, systems and controls should be improved along with proposals for appropriate improvements;

AML/CFT Policy

- A summary of the AML/CFT training imparted to officers and employees;
- Areas where the AML/CFT training program should be improved and proposals for;
- Number and types of customers, who are categorized as “high risk”;
- A summary on the progress in implementing AML/CFT action plans, like consideration the Annual Report by the BoD, assessment and review of training, any other issues relating to AML/CFT;
- Outcome of any audit reviews that was mandated by the Company in relation to AML/CFT policies, procedures, systems and controls;
- Outcome of any review or assessment of risks, policies, procedures, systems and controls.

AML/CFT General Principles

- ◇ Maintain appropriate AML/CFT procedure and controls for implementing the Policy;
- ◇ Apply appropriate CDD by:
 - Validate the identification of a customer **before** registering in the IT system, or making a one-off transaction;
 - Establish the beneficial owner(s) of any registered customer, and register them too, **before** executing any transaction for or on their behalf;
 - Build an **economic profile for corporate customers**, by obtaining the relevant information and supporting documents as described in the AML/CFT procedures;
 - Ensure the **full implementation of Customer Acceptance Policy**;
 - Undertake **EDD when dealing with PEPs, or high risk customers, or high-value transactions**, or for any reason there is a suspicion about a customer or transaction;
 - Perform **regular reviews for customers**, especially corporates, as defined in the Customer Monitoring Program Policy;
- ◇ Take reasonable steps to **recognize suspicious transactions**, and maintain a rigid procedure for **reporting them to the competent authorities** (FIU);
- ◇ Comply with the applicable, up-to-date **sanctions** imposed on persons (individual and corporates), organizations, and countries by UN, EU, OFAC, UK, and the instructions given by CBO;
- ◇ Maintain all customer/transactions related records for at least 10 years, or for longer period if the Law in the Oman requires.
- ◇ Cooperate with the authorities to the extent that is fully permitted by the applicable Laws in Sultanate of Oman.

6.1 KYC

- ◇ **Customer Acceptance Policy** – the Company has a policy in place which clearly defines the categories of persons (individuals, unincorporated bodies, or corporates) that are not accepted by the Company to become/be as customers. Apart of the not accepted categories, the Company has identified specific categories that impose a high money laundering risk on the Company and a specific approval procedure is detailed for customer acceptance in this case.
- ◇ **Customer identification** – it includes the collection of all relevant documentation and information, as detailed in the Company AML/CFT procedures, that will result not only in the identification of the customer but additionally in the creation of the economic profile of the customer, including the nature of the business activities the person (individual or corporate) is

AML/CFT Policy

engaged in.

At the opening stage, the Company screens the identification details through specific black/sanctions lists (as a minimum it uses the UN, EU, OFAC, UK, and CBO) for gathering more information from external sources, and assess the risk involved in the customer acceptance procedure.

- ◇ **Continuous monitoring** – the customers and their transactions are continuously monitored through the use of an appropriate AML system, so as to identify any unusual transactional behavior, or suspicious transaction and after thorough investigation to report these to the competent authorities (STR).
- ◇ **Risk management** – the Company apply effective KYC procedures, as detailed in the Company AML/CFT procedures, including adequate monitoring systems and controls, segregation of duties and authorities, staff training, and other relevant risk assessment and management measures.
- ◇ **Risk Assessment**- (as per Article 2 of AML/CFT -CBO 30/2016) The risk assessment and any information (Customer risk, Countries or geographic area in which customer operates or the place of origination or destination of a transaction, The nature of products, services and transactions offered and the delivery channels for products and services) shall be documented, be kept up -to -date and readily available for the Central bank of Oman to review upon request.

6.2 Ultimate Beneficial Owners

- The company apply due diligence measures, taking into consideration the results of the risk assessment as per the provisions of **CBO Article 34** of this law. Due diligence measures include the following:
 - a. Determine and verify the identity of customers based on reliable and independent sources, documents, data, and information issued by official authorities in the following cases:
 - 1.before establishing business relationship;
 - 2.before carrying out a transaction for a customer with whom it does not have an established business relationship the value of which is equal to or greater than the threshold specified by the supervisory authority, whether the transaction is executed in a single stage or in multiple stages;
 - 3.before executing a wire transfer for a customer with whom it does not have an established business relationship the value of which is equal to or greater than the threshold specified by the supervisory authority;
 - 4.when there is suspicion of a crime of money laundering or terrorism financing;
 - 5.when there are doubts concerning the accuracy or adequacy of obtained identification documents and information.
 - b. Identify and verify the identity of any person acting on behalf of the customer and seek proof of the authenticity of their agency according to applicable regulations.
 - c. Identify beneficial owners and take reasonable measures to verify their identity in a satisfactory manner. In the case of legal entities and arrangements, the ownership and control structure of the customer should be understood.
 - d. Know the purpose of the business relationship, and obtain related information appropriate.
 - e. Continuously update the data and information stipulated in paragraph(a) of this Article related to its customers and beneficial owners whenever necessary, or based on the timeframe specified by supervisory authorities.

AML/CFT Policy

6.3 Tipping Off

- Tipping off is prohibited under the provisions of **CBO Article 49**;
- We ensure that our officers and employees are aware of and sensitive to the issues surrounding and consequences of tipping off;
- We have policies, procedures, systems and controls to prevent 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 for making a STR to FIU instead of conducting CDD measures or monitoring. The CO/MLRO shall make and maintain record to the effect 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, he should not disclose this to the customer or any person;
- If the CO/MLRO finds that customer is hiding the fact or hiding the beneficial owner, he should not tell it to the customer, but refer the matter in Internal STR;
- 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;
- If the staff finds any letter from CBO / FIU, this should not be disclosed to any person/customer.

6.4 Record Keeping

The Company is maintaining all the documentary evidences about KYC, CDD, EDD, and transactions so as to be able to provide any kind of information about its customers and their transactions as and when these are required by Competent Authorities, regulators, Auditors, Customers etc.

The transaction-related records are kept for a minimum of 10 years, and are available for review as and when required; however, the records for transactions executed through third-party providers, e.g. Western Union, Transfast, Xpress Money etc., are maintained separately and are maintained indefinitely.

The documentation related to customer registration, KYC forms, or identification documents are either maintained in hard copy or in electronic form, for at least 10 years.

6.5 Know Your Employee

As part of “Know Your Employee” programme, the Company requests the following documentation as a minimum during the recruitment procedure:

- Resume or Curriculum Vitae (CV), detailing the personal and professional information;
- Educational qualification certificates, or professional certificates, duly certified or attested (where appropriate);

AML/CFT Policy

- Personal/professional background verification;
- Police clearance, where required.

For all positions reporting to the Board of Directors (controlled functions) or the General Manager, the prior CBO approval shall be taken before appointment.

The Human Resource Department shall check the antecedence of all new employees by checking their references when considering their application.

In order to ensure the integrity of the Company, HR and Line Managers must monitor their staff behaviour so as to identify and report to the CO/MLRO any situations that might be considered suspicious.

All managers/supervisors must know the staff in their department and report any unusual change in behaviour, substantial change in the financial situation or in the spending habits of the employees working directly under them to the CO/MLRO.

Compliance Department must check the name of the applicant or employee is not listed in OFAC, PEP and or Internal Watch lists. Every person in the Company will be screened against these lists annually.

An AML Compliance Undertaking will be taken from each and every employee of the company at the date of completion of the AML/CFT Training during Induction Programme.

Training

AML/CFT Training for all the Company members of staff is conducted regularly, with the minimum frequency of once per calendar year. The training programme includes the following as a minimum:

- **General information:** background and history related to anti-money laundering controls, what is money laundering and terrorist financing, stages of money laundering, why do criminals launder money and the necessity to combat the money laundering & terrorist financing issues within the financial system;
- **Responsibility of the employees** under the Oman AML/CFT Law, covering money laundering and terrorist financing matters, the need for obtaining sufficient evidence of identity, recognizing and reporting knowledge or suspicion of money laundering or terrorist financing, etc.;
- **Duties and responsibilities of the Compliance Officer/MLRO;**
- **Customer risk profile;**
- **PEPs;**
- **Potential effect** on the company, on its employees and customers, if there is any breach of AML/CFT Law or Regulations;
- Ways to **identify suspicious transactions;**
- Procedure for **reporting of suspicious transactions;**
- **Record keeping.**

Initial Training

- The CO/MLRO provides AML/CFT compliance and sanctions training to all new employees before allowing them to conduct or handle transactions;
- The CO/MLRO is responsible for ensuring that the training of each employee has been properly documented;
- To satisfy initial training requirements, each employee must execute one or more of the following:
 - a. Read the Compliance training materials and sign and date a training log;

Classification **Company Confidential**

POLICY

This document is uncontrolled if printed.

Doc ID POL-OM COMP002

Printed

Controller CO

Created 01/04/2015

Updated 20/02/2019

Owner CCO

Page 12
of 14

AML/CFT Policy

- b. CO/MLRO will obtain proof of training from the training provider or the employee will sign a training log;
- Each employee’s signed training log or other documentation of initial training will be retained for 10 years as legally required.

Ongoing Training

- The CO/MLRO and each employee who handles customer transactions is required to read, sign and date any correspondence that applies to compliance. The CO/MLRO will file this correspondence with the training records once all employees have read them and will retain them for 10 years;
- The CO/MLRO and each employee who handles or conducts transactions is required to read all compliance articles issued by the local authority or by other correspondents of the company. The CO/MLRO and each employee must sign or initial and date the article to document that they have read it. The CO/MLRO will file these articles with the training records once all employees have read them and will retain them for 10 years;
- All employees will attend the training course at least once a year. After the training course all employees will be given a “Knowledge Test” to complete and check their understanding and to score them accordingly. Employee’s scores on AML policy and procedures will also be used as one of the parameters for assessing their performance during their yearly appraisals;
- CO/MLRO will attend at least one training course a year conducted by a third party, independent from Lulu Exchange co LLC

Correspondent Relationship

- The Company shall gather sufficient information about the correspondent banks with whom they are going to enter into relationship with, through a structured questionnaire.
- The Company must obtain information about the correspondent banks ownership structure and management.
- The Company should pay attention to the quality of supervision by the relevant supervisory authorities when establishing correspondent relationships with Foreign Banks.
- Particular attention should be paid when entering into or continue a correspondent banking relationship with a bank incorporated in a jurisdiction in which it has no physical presence or located in jurisdictions that have been identified by FATF as “high risk jurisdictions”.
- The Company 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 into correspondent relationship with Shell Banks

7 Records

Document	Location	Duration of Record	Responsibility
KYC evidences	Branch/Warehouse	10 years minimum	Branch Manager/Warehouse in Charge
Employee documents	HR Manager	10 years	HR Manager

AML/CFT Policy

Classification **Company Confidential**

POLICY

This document is uncontrolled if printed.

Doc ID POL-OM COMP002

Printed

Controller CO

Created 01/04/2015

Updated 20/02/2019

Owner CCO

Page 14
of 14