Policy

Anti-Money Laundering and Counter Terrorist Financing

An Lulu Money Policy document

Document #	**POL-IE COMP001**
Created	**15/01/2018**
Updated	**24/04/2018**
Controller	**Compliance Officer**
Owner	**Chief Compliance Officer**

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

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

Classification **Company Confidential**

LuLu Money

Revision History

Date	Version	Author	Comments (including Review History)
15/01/2018	Draft 1.0	Christos Christou	Designed to meet the Legal and Regulatory Requirements of Ireland, and 3rd EU Directive on AML/CFT
21/01/2018	V 1.0	Christos Christou	I made changes to correct mistakes and comprehension/technical changes to meet BPMS Standards
24/04/2018	V1.0	Christos Christou	I have changed the name of the Company and the LOGO, after the name change approval

Contents

Contents

1 Summary

Purpose	The purpose of this Policy is to describe the fundamental principles that all members of Lulu Financial Services Ltd (Registered in the Republic of Ireland), trading as "**Lulu Money**" must fully comply with the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010, as amended by Part 2 of the Criminal Justice Act 2013, that transposes the EU's Third Money Laundering Directive (2005/60/EC) and its Implementing Directive (2006/70/EC) into Irish law, and the Criminal Justice (Terrorist Offenses) Act 2005.
Scope	The Policy applies to Lulu Money ("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-IE Sanctions Policy
Procedures	PRD-IE AML/CFT Procedures
Work Instructions	WI-Compliance Investigations
Forms	FRM-IE iSTR
Other	

3 Definitions

Term/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 and Money Laundering Reporting Officer
Company	Lulu Financial Services Limited, trading as "Lulu Money", its branches, associates, and or 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 transaction during an investigation procedure.
FIU	Financial Investigation Unit
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 – an act intended to have the effect of making any property a) that is, the proceeds obtained from the commission of an indictable offence under the laws of Ireland, or of any conduct which if it had occurred in Ireland would constitute an indicable offence under the laws of Ireland, or b) that in whole or in part, directly or indirectly, represents such proceeds, not to appear to be or so represent such proceeds.
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.
CBI	Financial Regulator under the Central Bank of Ireland
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 – a) the provisions or collection, by any means, directly or indirectly, of any property (i) with the intention that the property be used, or (ii) knowing that the property will be used, in whole or in part, to commit one or more terrorist acts (whether or not the property is actually so used); or b) the making available of any property or financial (or related) services, by any means, directly or indirectly, to or for the benefit of a person knowing that, or being recknless as to whether, the person is a terrorist or terrorist associate; or c) the collection of property or solicitation of financial (or related) services, by any means, directly or indirectly, for the benfit of a person knowing that, or being reckless as to whether, the person is a terrorist or terrorist associate.

4 Introduction

The Company is operating under license from the CBI as a Payment Service Provider (PSP); 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 appointed a CO/MLRO to design, implement, and manage this AML/CFT Compliance and Sanctions Program.

The Company has designed a number of policies, including the AML/CFT Policy and other Compliance Policies, that must be strictly followed by all the members of staff of the Company.

5 Policy Statement

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

- To comply with the provisions of the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010, as amended by Part 2 of the Criminal Justice Act 2013, that transposes the EU's Third Money Laundering Directive (2005/60/EC) and its Implementing Directive (2006/70/EC) into Irish law;
- To comply with the Criminal Justice (Terrorist Offenses) Act 2005;
- To abide by the rules issued from time-to-time by the CBI and EU, and to assist the regulatory authorities in combating Money Laundering and Terrorist financing;
- To abide by the FATF recommendations and Wolfsberg Group Guidance, especially those related to KYC and Remittances;
- To ensure that company and its staff will not knowingly assist anyone to launder the proceeds of drugs sales, illegal businesses, embezzlement, terrorism or other acts prohibited as predicative offences in Ireland;
- To effectively meet all the requirements of "Know your Customer" process;
- To comply with all the sanctions regimes and implement automated systems to check and validate any transactions that may be related directly or indirectly to a sanctioned individual or entity;
- To design and implement appropriate internal AML/CFT policies, procedures, and controls.

6 Policy Notes

6.1 Organizational Structure

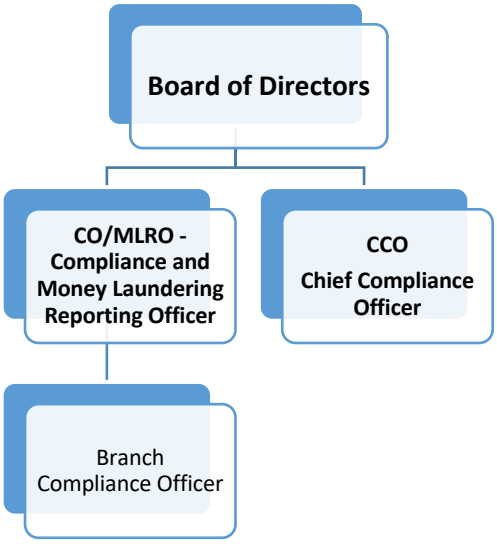
The Board of Directors of the Lulu Exchange Holdings LLC (the Holding Company) has appointed a CCO to direct and manage the Compliance Function within the Group; the Board of Directors of the Company has appointed a CO/MLRO to manage the customers and transactions executed within Ireland; based on these appointments, the compliance department has the following structure:

- **Chief Compliance Officer (CCO)** – heading the Group Compliance Department and directs the compliance function for the Group; the CCO reports directly to the Board of Directors of the Holding Company, and receives periodical reports by the CO/MLRO for the Company's compliance level;
- **CO/MLRO** – is responsible to manage the compliance function within the country; the CO/MLRO reports directly to Board of Directors of the Company, but he receives consultancy by the CCO for any guidance required; reports to the CCO periodically for the compliance level of the Company;

- **Branch Compliance Officer** – is responsible to implement the AML/CFT Policy in the Branch (where applies), and report any suspicion, via the formal iSTR form (FRM-IE iSTR), to the CO/MLRO.

Special Note: The Company is appointing the Branch Managers as Branch Compliance Officers (BCOs) as an additional control measure; however, the role to implementing the policies and procedures within the Operations and report any suspicions directly to the CO/MLRO (iSTR) is an obligation of all employees, and should NOT at any point in time communicate any of their suspicion to the customer/person/entity involved in the suspicion.

FUNCTIONAL CHART OF COMPLIANCE DEPARTMENT



Responsibilities for the AML/CFT Compliance and Sanctions Program execution:

- Board of Directors:
  - Approve the AML/CFT Compliance and Sanctions Program;
  - Approve any amendments related to AML/CTF and or Sanctions Policies;
  - Appoint the CO/MLRO;
  - Review the Quarterly and Yearly Compliance Report prepared by the CO/MLRO, and give instructions for further actions and activities to comply with the Legal and Regulatory Framework of Ireland;
  - Approve the Compliance budget so as to implement the AML/CFT Compliance and Sanctions Program.

- Chief Compliance Officer - CCO
  - Assist the CO/MLRO in the design of the AML/CFT Compliance and Sanctions Program;
  - Assist for any amendments related to AML/CTF and or Sanctions Policies;
  - Manage the performance of the CO/MLRO;
  - Review the Quarterly and Yearly Compliance Report prepared by the CO/MLRO, and give guidance to the CO/MLRO about the proper implementation of the Compliance controls;
  - Train the CO/MLRO and assist in the implementation of proper AML/CFT Training.

- CO/MLRO:
  - Identifying, documenting and assessing the compliance risks associated with the Company's business activities, including the development of new products and business practices, and reporting these developments to the BoD;
  - Developing new practices and methodologies for the measurement of compliance risk;
  - Identifying, with the assistance of the BoD or external legal advisors, the regulatory framework which governs and or affects the operations of the Entity, including the creation and maintenance of an up to date register of the existing regulatory framework including evaluation of compliance;
  - Providing immediate information to the senior management and the BoD on any identified breaches of the AML/CFT Policy, or of the applicable statutory and regulatory framework and on any deficiencies in complying with the provisions of the country statutory and regulatory framework; Creation of country compliance procedures, alignment with the Legal and Regulatory requirements of Ireland and Lulu Financial Group Compliance Policies;
  - Maintaining effective communication with the local regulatory authorities.
  - Developing, documenting, implementing and executing a comprehensive AML/CFT Compliance and Sanctions Program;
  - Is the recipient of all the Critical Incident Reports and Internal Suspicious Transactions Reports (iSTRs), and takes any measure to assess and manage the risks related to these in the most appropriate manner, so as to avoid/mitigate any risks imposed on the company;
  - Providing reports on a regular basis, as directed or requested, to keep the BoD informed of the operation and progress of regulatory compliance efforts;
  - Ensuring that Regulatory Compliance Policies and Procedures are followed by the operations and departments;
  - Conducting ongoing monitoring of the country's' operations and activities and evaluating associated regulatory compliance risks;
  - Being continuously updated for the country's Legal and Regulatory Environment;
  - Communicating new guidelines issued by Regulators to various departments of the Company, thereby ensuring compliance with the guidelines issued;
  - Making sure that the Company’s Compliance Policies and Procedures, including the AML/CFT Policy and Procedures, are updated with the latest Legal and Regulatory requirements of the country, in line with the approvals by the BoD;
  - Ensuring that all employees with the company are trained in regulatory compliance-related matters and are performing their functions in compliance with the rules, regulations and firm's internal policies;
  - 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 and Procedures;
  - Ensuring to have records on all training conducted on AML/CFT for the employees within the country;
  - Conducting regulatory compliance reviews on an ongoing basis, and monitors the CBI and or JFIU examination audits;
  - Liaise with the CCO and all Departments, either at Global or Regional level, for any queries, or new developments that affect the overall business of the Company;
  - Prepare and ongoing monitor the Compliance Framework testing activities within the company;
  - Providing support and proper guidance to Departments, including operations, that have queries related to regulatory compliance;
  - Report any suspicion, for AML/CFT or Fraud, to the FIU as per the procedures.

- Branch Compliance Officer:
    - Takes instructions and reports to the CO/MLRO all matters regarding all AML/CFT;
    - Is fully responsible for keeping the branch staff informed at all times about the Company's Policy and Procedures related to the AML/CFT;
    - Is required to conduct periodic meetings in the branch to update the staff about any change in the regulations or new guidance issued by the Company related to AML/CFT;
    - Is fully responsible for implementing, verify, and authorize as the first level all the transactions as per the Company SOPs, and related to the AML/CFT;
    - Is responsible for filing and safekeeping of all transaction documents related to AML/CFT for a period of minimum six (6) years after the termination of the customer transaction, and make these documents available whenever required by any competent authority, or for audit;
    - Apply, verify, and authorize all KYC procedures executed in relation to the registration and maintenance of customers;
    - Authorize the correct collection of identification documents of customers, especially the corporate customers, and apply Due Diligence in the maintenance of all customers' identification procedures;
    - Perform Enhanced Due Diligence(EDD) and risk assessment for transactions considered as "high value," or when dealing with "high-risk customers," or whenever this transaction is considered to be of high risk;
    - Is responsible for identifying any unusual, or suspicious, or structured transactions, or suspicious customer behavior and report them immediately to the CO/MLRO, via the "FRM-IE iSTR" form.

6.2 Know Your Customer (KYC) Policy

- The Customer Registration procedure is mandatory for all transactions, i.e. inward or outward remittances, and foreign currency money exchange;
- The formal Customer Registration procedure is also mandatory for all transactions executed in the name of and on behalf of a Corporate (legal entity), including the owners, managers, authorized persons, and beneficial owners;
- All registered customers (physical and legal) will be identified by a Unique Identification Number.

6.3 Customer Acceptance Policy

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

- The Company 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 Company services for ML, or TF, or other criminal activity.
- The Company 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 refuses to provide his identity card or passport for verification, the transaction shall be refused.

As per the customer acceptance policy of the Company, the staff will follow the below guidelines:

- The Company deals with customers that have formally identified at all times;
- The Company does NOT deal with non-face-to-face customers;
- The Company does NOT deal with non-profit organizations, except where these organizations have taken the written approval from the Ireland government;
- The Company does NOT deal with “shell banks”, “shell companies”, or “unidentified individuals”;
- The Company does NOT deal with any type of crypto-currency, or in a currency that is NOT recognized and accepted by the CBI.AML/CFT Risk Factors

6.4 PEP Client Acceptance Policy

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 approved as these individuals are considered by default as high-risk customers, identified by the AML System and categorized by the automated Risk Categorization Model in the AML System, and are flagged as “PEP” in YOM.

Customer Registration will be established with all PEPs only after getting approval from the CO/MLRO. If any existing customer, or the beneficial owner of an existing corporate customer, has subsequently found to be linked to or has become PEP, then the relationship will be continued only after prior approval from the CO/MLRO.
PEPs are 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 EUR1,000. In case of any suspicion, then an STR has to be filed with the FIU.

6.5 AML/CFT Risks

The Company has implemented an appropriate Customer Risk Categorization methodology in order to identify, calculate, score, and categorize the customers; this Customer Risk Categorization considers the following factors:

Country Risk

The Company has designed a Sanctions Policy, reference to “**POL-IE Sanctions Policy**”, by which periodically identifies different sanctions and other data related to countries and territories; this data include the Transparency International Index, the FATF high-risk and NCCT list, different Regulators’ specific instructions related to countries etc. After the identification of these risks and data, the Company categorizes the different countries to the following categories:

a) Non-compliant
b) High risk
c) Medium risk
d) Low risk

Accordingly it applies this categorization to the Customer Risk Categorization methodology/model in its AML System, as this is explained below.

Customer Risk

The Company serves a diversified customer portfolio, with individuals and corporates from different industries, profession types, residence types etc.; hence, the different risks associated with the "customer" are identified through our Customer Risk Categorization methodology/model and used in our Risk Scoring model in the AML System, as this is explained below.

Transaction Risk/Distribution Channel Risk

The Company has stated in this Policy that the primary delivery channel is the Branch; however, based on the technological advancement and heavy investment in FinTech, the Company offers alternative delivery channels AFTER it has formally identified the individual or corporate. Thus, the Customer Risk Categorization methodology/model used considers the following risk variables based on the transaction types:

a) Cash transactions – amount variables differing, e.g. >=EUR1,000, or EUR1,000<>EUR10,000 etc.
b) Foreign currency – transactions in foreign currency with amount variables differing (as above)
c) Electronic channels – transactions executed via bank transfers with amount variables differing (as above)

Product Risk

The Company is operating as a PSP; hence, by default it offers two distinct products only to its customers – the the money transfers (remittances) and foreign currency exchange (as a supplementary service where applicable). It is important also to note that, based on our Operations Procedure when a customer is registered properly with us, with full identification details and other evidences, we can issue a "gold card" which directly is used as "loyalty card" for fast tracking during their transactions execution process. In this respect, the Customer Risk Categorization methodology/model and used in our Risk Scoring model in the AML System, as this is explained below.

AML Risk

The Company is using an AML System for the customer screening and transaction monitoring controls; therefore, there are alerts generated for watchlist and PEP matching of customers and based on these alerts we consider flagging the customers as "high risk" by default if there is any such alert confirmed. In this respect, the Customer Risk Categorization methodology/model and used in our Risk Scoring model in the AML System, as this is explained below.

6.6 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 necessary Regulatory Authorities' approvals will be taken (where applicable).

The HR Department will also 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 also requests from the CO/MLRO to execute an independed background check for every employee from any sources that are available with the CO/MLRO, and any information found should be communicated confidentially to the HR Department with 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. Training is either provided by the Company internally, or through the Lulu Financial Group Chief Compliance Officer, or by other external firms engaged for this purpose. All the records related to training and employee undertaking are collected and stored. Furthermore, the Company has adopted a strategy to **create a mandatory AML/CFT Refresher Course for every employee minimum twice a year.**

7 AML/CFT Risk Management and Risk-based Approach

The Company has introduced a thorough risk management approach while executing business; it extended its risk management strategy to cover Market Risk, Currency Risk, Rate Fluctuation Risk, AML/CFT Risk and others. In order to manage the risk related to AML/CFT, coming from the customer transactions mainly, The Company has decided to implement the following methodology:

7.1 Customer Risk Categorization

The Company has designed a Customer Risk Categorization methodology/model which has been incorporated in its AML System; based on this model, the customer (for all types of transactions) are categorized into "High Risk", "Medium Risk", and "Low Risk" categories. The model is taking into consideration the following risk factors:

a) **Country Risk** – it considers the country-related static data provided by the KYC details registered, i.e. "nationality", "residency", "ID issuing", "beneficiary nationality", "beneficiary residency", "beneficiary bank's residency"; it compares the risk based on the country categorization executed and published within the Sanctions Policy of the Company.
b) **Customer Risk** – it considers the static data registered for the customer provided in the KYC procedure, i.e. the "profession" or "industry type", the "identification document" if missing or expired, the type of residency ("resident", "non-resident", "tourist", "diplomat" etc.).
c) **ML Risk** – it considers any alerts generated for matching with sanctions or PEP public data.

d) **Product Risk** – it considers the type of products that are used by the customer, i.e. foreign currency exchange, or one-off remittances etc.
e) **Transaction Risk** – it considers the aggregated amounts of cash, and foreign currency transactions executed by the customer within a period.

The customer is assigned a risk category, which is re-calculated at frequent time intervals and whenever there is a transaction executed; dormant customers are NOT re-calculated until they execute a transaction.

8 Customer Due Diligence

The customer due diligence executed is based on the type of risks identified and the category of these risks; simple due diligence is exercised for low and medium risks, whereas enhanced due diligence is exercised for high risks.

8.1 Customer Due Diligence

The CDD measures taken for every transaction are:

a. **Identification and Verification of identity** – new customers (not registered) are identified by collecting the original identification document, whereas complete identity verification activities are executed for all customers (new and existing);
b. **Identify and verify the UBOs** – the ultimate beneficial owners of corporates or unincorporated bodies must be identified completely and verified from any available public sources;
c. **Business relationship** – the purpose of the transactions should be established at all times, even if it is an occasional transaction;
d. **Third-party transactions** – identify and verify the person executing the transaction and on whose behalf, this is executed.

Special Notes:

- transactions or other types of business relationships with persons from, or corporates registered in, jurisdictions identified by FATF as "non-compliant" should be done only after EDD measures taken;
- collective or linked transactions - remittance transactions exceeding EUR10,000 or foreign currency exchange transactions exceeding EUR10,000 – should be done only after EDD measures taken;
- "ultimate beneficial owners" are individuals that possess or control more than 10% of the shares, or units, of a corporate or unincorporated entity;
- third-party transaction executors must be identified formally using an "authorization letter", or a "Power of Attorney", or "Special Authority Letter" in addition to the formal identification document presented as an individual;
- identification documents in a foreign language, other than the official Ireland languages and English, should be translated by an authorized body and notarized by appropriate governmental bodies.

8.2 Establishing the business relationship

Further to the identification process, we have to understand the nature of the business/profession/employment/industry the customer is engaged in; this data is recorded in YOM, and the AML System will apply the appropriate risk scoring rating automatically. The Customer Risk Categorization methodology/model will apply automatically the risk score and category of each customer, thus considering the level of CDD applicable.

8.3 Maintenance of Customer Information

Since the type of business relationship that the Company has with its customers is "transaction-based", and no account is maintained, the data and information of the customer and the beneficiary are continuously maintained. The front-line associates must request the identification of the customer, the real purpose of the transaction, and the relationship between the sender and beneficiary (applicable in remittance transactions only) for every transaction they execute.

Natural Person

The identification information that must be collected and logged in YOM for a physical person includes, but not limited to:

a. Full name, as this is written in the identification document;
b. Date of birth;
c. Place of birth;
d. Nationality;
e. Identification document (valid, original), issuing country, and number

Note – a copy of the original, valid identification document is taken, stamped as "original verified", and signed by the front line associate; this copy is maintained with the "Customer Registration Form" signed by the customer as per the records retention period stated below.

The valid identfication documents that can be accepted are:

1. **Identity Card** – issued by a reputable government body, containing photograph for verification;
2. **Travel Document/Passport** – containing biodata and issued from a reputable government body;
3. **National Driving License** – issued by a reputable government body, containing photograph for verification.

The front line associates must additionally collect the residential address of the registered customers, or beneficiaries, or persons that execute an occasional transaction; there is a requirement of verifying the address vary according to the type of residency.

Legal Persons and Unincorporated Entities

For corporates or unincorporated entities, the Corporate Booklet of the Company should be completed fully and include all the data that is mandatory to be entered in YOM; these data include the registration and registered address of the corporate or unincorporated entity, as well as the personal data of the ultimate

beneficial owners, managers, and authorised persons that will execute transactions on behalf of the corporate or unincorporate entity.

The information that have to be collected, as a minimum, and logged in YOM is:

a. Full name, as in the registration document;
b. Date and place of Incorporation/Registration;
c. Registration and or Incorporation number;
d. Registered Office address – must be verified in the place of incorporation/registration country;
e. Primary Business Address.

The data should be validated from the following documents collected as a minimum:

1. **Certificate of Incorporation, or Registration;**
2. **Memorandum and Articles of Association** (where applicable);
3. **Corporate Governance – ownership and corporate structure (management)**.

Beneficial Owners

The Ultimate Beneficial Owners (UBOs) of a Corporate or an Incorporated Body are the individuals who hold singly and collectively a stake of 10% and above, or controls the shareholding interest of more than 10%.

All the UBOs must be identified, and proper CDD measures have to be taken, including the maintenance of the physical person's Customer Information as described above.

Non-Profit Organizations

It is the Policy of the Company NOT to deal with any Non-Profit Organizations, either local or international.

Exceptions – there may be cases whereby for humanitarian reasons the Company will allow a transaction to be executed through a Non-Profit Organization; **this requires the prior approval of the Compliance Officer.**

8.4 Simplified Customer Due Diligence

The Company applies Simplified Customer Due Diligence (SCDD) to the following types of customers:

1. Financial Institutions, licensed by the CBI or other Regulatory Body in Ireland;
2. Government, or semi-government body/department;
3. Financial Institutions licensed in a reputable jurisdiction;
4. A Corporate that is listed in a reputable Stock Exchange.

The identification of the above institutions is done by:

a. Official Registration or Identification evidence;
b. List of Authorized Persons, duly verified by the respective institution;
c. Evidence of licensing/Listing (where it applies).

Additionally to the institutions stated above, the Company applies SCDD to customers that execute foreign currency exchange of an amount **LESS** than EUR10,000 or equivalent.

8.5 Enhanced Customer Due Diligence

The Company executes EDD on every customer of, and every transaction for, the following categories:

1. **High Risk customers** – when a customer has been categorized as a "high risk" by the Customer Risk Categorization methodology/model;
2. **Customers NOT physically present** – even though the Company does NOT allow transactions to be executed WITHOUT the physical presence in the Branch, there are transactions executed through alternative delivery channels, e.g. Electronic means or Applications;
3. **PEPs** – when a transaction is executed by a PEP;
4. **Transactions to/from high-risk jurisdictions** – the list of countries and jurisdictions are published based on the Company's Sanctions Policy;
5. **Transactions ABOVE the limit threshold (HVT)** – the transactions ABOVE the amount of EUR10,000 will be always subject to documentary verification of the source of funds, e.g. a bank statement, or bank transfer slip etc.

9 Ongoing Monitoring

The Company has set appropriate procedures in order to monitor the customer data, information, and transactions; in this respect, it has set rules and scenarios in its AML System to automate the transaction monitoring process, but as a Policy the Company has set the following:

a) **Keep the customer documentation and data updated** – the Company reviews the data in YOM and maintains the required documents so as to make sure they are up-to-date;
b) **Execute thorough transaction monitoring** – the AML System is set up to identify unusual transaction behavior, based on data and statistics collected (customer profiling), and gives a different alert according to the risk area identified to the CO/MLRO in order to investigate and decide if suspicious;
c) **Execution of EDD** – the Company has set a limit of EUR10,000 for any kind of transaction so as to execute EDD, therefore requires a valid evidence of Source of Funds (SoF), other possible evidences for the transaction purpose, and relationship between sender-beneficiary (for remittances ONLY);
d) **Assess continuously the controls to be adequate** – based on the type of product sold, and the business model it follows, the Company is considering the adequacy of controls imposed and adapts them in case there is anything identified;
e) **Frequent review of correspondents or agents** – the Company has a Policy to review the correspondents (other FIs having either remittance arrangements or purchase/sale of foreign currency agreements) **at minimum once every year**, or sooner if the CO/MLRO assesses to be exposed to higher AML/CFT Risk. In this respect, the Company will collect additional answer using an AML/CFT Questionnaire or other evidences required.

10 Financial Sanctions

The Company has issued a separate Policy related to Financial Sanctions, reference "**POL-IE Sanctions Policy**", and the relationship of those is relevant to the measures taken by the Company during executing transactions. In the Company's procedures, the automated scanning of names to identify possible matches with designated names is mandatory for all transactions.

The Company is using the publicly available sanctioned entity lists of UN Security Council OFAC SDN list, EU Consolidated Sanctions List, and UK-HMT Sanctions List.

11 Terrorist Financing

The Company is abided by the UN Security Council Resolution 1373 (2001) whereby, and it takes every necessary step to prevent the financing of terrorism. The AML System is configured to download and maintain the UN lists related to the individuals and organizations that are subject to UN financial sanctions, and is filtering all names within a transaction to find if the customers or beneficiaries are related to terrorism. If there are any matches found, then a thorough investigation is executed so as to identify and verify properly these persons and stop any transactions to terrorists.

12 Reporting of Suspicious Transactions

12.1 Transaction Screening and Monitoring

The Company uses modern technology for on-going transactions monitoring. It configured in its AML System rules and scenarios, and are applied for sanction screening 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.

12.2 iSTR

An Internal Suspicious Transactions Report (iSTR) is raised by the Branch staff, or Internal Auditors, to the CO/MLRO in case of any suspicion that has come to their attention. All the iSTR are logged with the relevant supporting documents/evidences of suspicion.

The Company has designed and published an iSTR form, "**FRM-IE iSTR**", which every member of staff, irrespective if working in the Branch or Head Office, could use to notify the CO/MLRO for any suspicious. The member of staff can also inform the CO/MLRO about any suspicion by phone, or email.

12.3 STR

The Company has implemented an automated control of the customer profiling and transactional monitoring through an AML System, therefore any possible violation of the defined rules provide an alert to the Compliance Team.

All the suspicious cases which are reported through iSTR, or identified through alerts from the AML System, or identified independently from the CO/MLRO, are reviewed and investigated in depth, taken into consideration the provisions of the the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010, as amended by Part 2 of the Criminal Justice Act 2013, that transposes the EU's Third Money Laundering Directive (2005/60/EC) and its Implementing Directive (2006/70/EC) into Irish law, and the Criminal Justice (Terrorist Offenses) Act 2005, and any evidenced suspicion is reported by the CO/MLRO to the FIU.

If the CO/MLRO is notified by the FIU NOT to execute any transaction, for the reasons of suspicion related to money laundering or terrorist financing, then the CO/MLRO will give specific instructions to the Operations for NOT proceeding with the specific transaction, block the customer, and other required actions so as to comply with the FIU requirements.

12.4 Tipping Off

- Tipping off is prohibited under the provisions of the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010, as amended by Part 2 of the Criminal Justice Act 2013, that transposes the EU's Third Money Laundering Directive (2005/60/EC);
- Since it is an offence based on the Law, the Company ensures that the 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 or the CCO, 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 CBI, or FIU, or Police these should not be disclosed to any person outside the Compliance Team or customer.

13 Record Keeping

The objective of record keeping is to ensure that we can provide necessary information about customers, and their transactions details at any given time or as per the request of competent authorities, CBI, FIU, Law Enforcement Agenecies, Courts, or Auditors/Examiners.

All the receipts, records and documents are retained for a minimum period of six years AFTER the end of the business relationship wth the customer. These records can be stored as hard or soft copy, and strict process of document control is applicable, even after the end of the six-year period from the transaction date.

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.

14 Correspondent Relationship

14.1 Correspondents and Arrangements

The Company will open and maintain banking and other contractual relationships with financial service providers around the world, therefore it is important to know and understand the risks that are involved in such relationships. Therefore, the CO/MLRO, as part of the procedure, will review and assess the following factors:

- 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 "**FRM-IE Compliance Assessment on Third Party Agreements**", as per the "**PRD-IE Compliance Assessment on Third Party Agreements**" and approve or reject such a relationship based on the risk assessment results.
- The approval of the Regulators is obtained, if required).

14.2 Appointment of Agents

The Company may decide in future to appoint Agents for execution of remittance transactions, using the Company's POS tools; in every case of this Principal-Agency Agreement, the following must be maintained as a minimum:

- The CO/MLRO shall gather sufficient information about the agent with whom the Company is going to enter relationship with, through a structured questionnaire.
- The CO/MLRO must obtain information about the agents' ownership structure and management.
- The CO/MLRO should pay attention to the quality of supervision by the relevant supervisory authorities, gather all the details of the licensing (if any), and assess the market risks associated with its business before establishing correspondent relationships with foreign Banks.
- The CO/MLRO should establish that the agents have due diligence standards and employ due diligence procedures with respect to transactions carried out through the accounts. **The minimum prevailing standards will be those of the Company.**
- The Company will not enter agency agreements with any Shell Banks, or Shell Companies.
- The CO/MLRO must assess the risk involved in such a relationship, through the completion of the form "**FRM-IE Compliance Assessment on Third Party Agreements**", as per the "**PRD-IE Compliance Assessment on Third Party Agreements**" and approve or reject such a relationship based on the risk assessment results.
- The CO/MLRO must continuously monitor the transactions executed by the agent, whereas the CO/MLRO must execute yearly risk assessments for every agent, as a minimum, or earlier if required.
- The pre-approval of the Regulators must be obtained (where required).

THE APPROVAL OF THE CO/MLRO AND SENIOR MANAGEMENT OF THE COMPANY IS REQUIRED IN ORDER TO ENTER INTO OR MAINTAIN AN AGENCY RELATIONSHIP.

15 Staff Training

The Company is committed to the training and development of its members of staff, not only because it is mandatory by the Regulators, but because it is embedded in its business excellence model and values.

All the staff of the Company are trained on AML/CFT as follows:

- **MANDATORY –** Basic Principles of AML/CFT during the induction period, including the AML/CFT Policy and Procedures;
- **MANDATORY –** How to identify and report suspicious transactions, through the formal iSTR form, during the induction period;
- **MANDATORY –** refresher AML/CFT Training to all members of staff, minimum once per year;
- **MANDATORY –** Advanced AML/CFT Training to all Branch Management and Operations Management, once per year, so as to cover the different risk areas and risk assessment and reporting requirements;
- **MANDATORY –** all AML/CFT related Policies, Procedures, Forms, Templates, Work Instructions etc. are passed to every member of staff through an electronic document management system (eDMS) and they are obliged to read and keep updated with new developments and requirements; the CO/MLRO monitors their compliance to the reading requirements.

The Company is also looking into the options of implementing an eLearning Platform for AML/CFT Basic Principles, in order to automated the learning process of its employees and maintain a continuous learning culture embedded all through.

16 Reporting

16.1 Statutory Reporting

The CO/MLRO must ensure that the statutory reporting requirements under the AMLO or other Regulatory Requirements are strictly followed.

16.2 Internal Reporting

The CO/MLRO must prepare a complete and evidenced report to the BoD every quarter, detailing the different actions/activities executed during the reporting period and related to AML/CFT; the report is presented to the BoD for discussion, and for acknowledgement of risks and mitigating measures. The BoD may give specific written instructions to the CO/MLRO for actions to be taken in order to comply fully with the Legal and Regulatory Framework described in the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010, as amended by Part 2 of the Criminal Justice Act 2013, that transposes the EU's Third Money Laundering Directive (2005/60/EC) and its Implementing Directive (2006/70/EC) into Irish law, and the Criminal Justice (Terrorist Offenses) Act 2005.

The Company also authorises the CO/MLRO to give a brief weekly report to the CCO, defining the different risk areas and activities the Compliance Function has executed; this report is copied also to the Management of the Company, and is considered as an overall guidance towards the appropriate AML/CFT risk mitigation procedures and controls.

17 Records

Document	Location	Duration of Record	Responsibility
KYC evidences	Branch/Warehouse	7 years minimum	Branch Manager/Warehouse Manager
Employee documents	HR Manager Office	7 years	HR Manager
Training attendance sheet	CO/MLRO Office	indefinitely	CO/MLRO