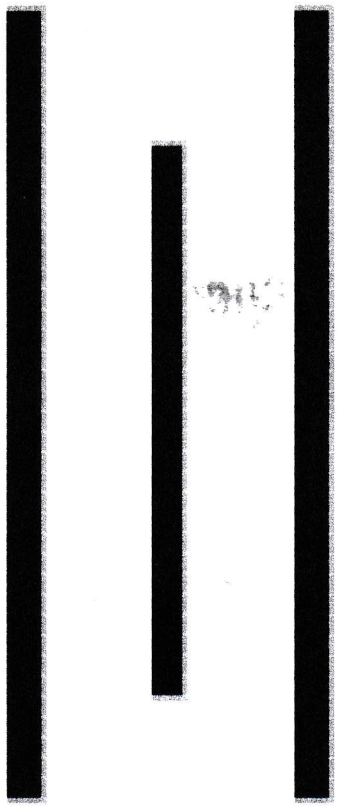
Anti-Money Laundering (AML) Policy



EmerioBanque©

April 2020

Revision History & Version Control

#	Base Version	Date	Name of Author	Name of Reviewer	Review Date	Brief description about the change incorporated
1						
2						
3						
4						

Document Classification: **Internal**

Approvals

	Name:	Date:	Signature
Forwarded By:			
Reviewed By:			
Supported By:			
Approved By:			

Table of Contents

1. Introduction

1.1. Overview

Money Laundering (ML) is considered as a potent threat to financial system of all countries. The magnitude of its damage extends to a larger dimension in the form of loss of sovereignty and image of a country. This has been now recognized globally and has culminated in concerted efforts to fight against this ultra-criminal activity by way of enactment of stringent laws, regulations and measures aimed at securing financial systems against money laundering.

The financial activities of most countries are still predominantly ruled by cash based transactions or transactions emanating from non-account holders. There is a significant part of global economic activities which are run through informal channels and mechanism which are not in the direct control of law enforcement agencies. However, banks and FIs are at some level used by these informal channels to move/route funds between countries.

There is indeed a need to monitor, control and act against the practices that are directly helping individuals, group and organizations to evade taxes, drugs/human trafficking, finance terrorism pose threat to global economy.

The bank is committed to:

- Meeting its international regulatory obligations in the identification, treatment and management of ML/TF risk.
- Protecting the bank from reputational risk and breaches of regulatory requirements that may lead to sever fines and penalties.
- Safeguarding the bank, its customers and employees from becoming a victim of, or unintentional accomplice to, ML/TF activities.

1.2. Definition ML/CFT

Money Laundering is an activity involving transaction/or series of transactions that is designed to disguise the nature/source of proceeds derived from illegal activities, as defined in the Money Laundering Prevention Act 2010, United Kingdom, which may comprise drug trafficking, terrorism, organized crime, murders, fraud, etc.

It is important for all employees of the Bank to be conversant and familiar with the ML process (described below) as they must be vigilant all the times and should any of the aspects involved in ML process surface our business they must be able to identify the warning signs and take appropriate actions.

Placement: The first stage is successfully disposing of the physical cash received through illegal activity. The criminals accomplish this by placing this into a financial institution.

Layering: The second stage concentrates on separation of proceeds from criminal activity through the use of various layers of monetary transactions. These layers are aimed at wiping audit trails, disguise origin and maintain anonymity for people behind the transaction.
E.g. Fraudulent letters of credit transactions, over pricing invoicing for goods transshipped from another country, using high value credit cards to pay for goods/services and accounting for the credit card invoices with balances held in offshore banking secrecy havens, etc.

Integration: The final link in ML process is sometimes called the integration stage. This occurs when the laundered or cleaned up money is legitimately brought back into financial systems operated by end user and when it is safe and insulated from enquiry by any agency with a legitimate reason for querying the existence of money. E.g. Loan back technique or loan-default technique where the lender bank seeks to recover its assets (loans to money launders) by attaching the securities held by bank which exist in the form of dirty money.

1.3. Purpose

This EmerioBanque AML Policy is based on the requirement of the Sanctions and Anti-Money Laundering Act 2018. Also, this policy incorporates agreed international rules and regulations and best practices, which directs EmerioBanque's banking activities to proactively comply with AML prudent practices among its stakeholders.

This policy's purpose is to establish governing standards to insulate the bank from being used as a component of financial system to launder money.

In the light of the above the purposes of the policy are:

a) To enable the bank to conduct clean business conforming to standards set by the industry, laws and regulations of the country/governing authorities.
b) To follow, the internationally accepted standards used for KYC compliance, as far as practical.
c) To report and take suitable actions, upon detecting the suspicious activity involving shades of money laundering as directed by the Financial Conduct Authority United Kingdom or any other laws formulated from time to time.
d) To make employees and customers aware about the seriousness of the impact of ML activities.
e) To set-up administration processes with the Bank to implement the set AML standards.
f) To comply with applicable laws in United Kingdom with reference to ML and adhere to standards accepted internationally by the financial world on the subject, as far as practical.
g) To provide the knowledge to identify AML/CFT transactions.

h) To make bank's staff aware of the AML/CFT policies and practices.
i) To avoid the opening of anonymous, UN sanctions list and fictitious accounts.
j) To provide the knowledge to staff to verify the identity of prospective customers before they are allowed to established relationship.

1.4. Scope

The four basic tenets of AML have been covered in this policy. They are:

a) Know Your Customer (KYC)
b) Risk Assessment of Accounts
c) Accounts Review
d) Suspicious and Large Value Transaction Monitoring and Reporting

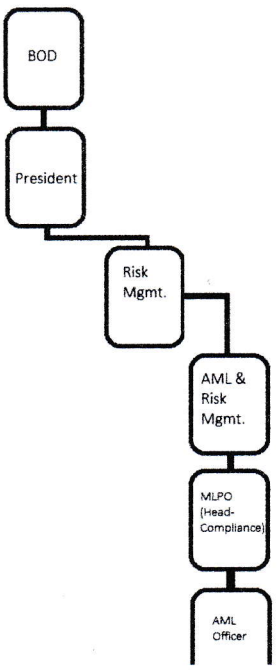
This policy also intends to increase awareness of ML activities amongst the staff, customers and general public and its ill effects and also effectively counter/guard against ML at all times.

There is a specific law "Sanctions and Anti-Money Laundering Act 2018" prevailing in United Kingdom. Financial Conduct Authority has formulated guidelines on KYC. Considering the sensitiveness of the matter on global arena the Bank has developed this Policy in order to be proactive in dealing with issues related with ML within the preview of the prevailing international laws and guidelines.

Compliance and willing adoption of this policy will be the primary goal while implementing it. All EmerioBanque employees and affiliates must comply with this policy.

2. Governance for AML/CFT

Governance structure assigns responsibilities for the design of the banks AML/CFT implementations and monitoring structure and overall accountability for results. To align with our business requirements, it incorporates guidance from global standards, Central Bank of United Kingdom circulars and directives and elements consistent with evolving best practices. A key element of our compliance governance structure is as below:



2.1. Roles and Responsibilities

The Section below details the various roles and responsibilities of governance structure for AML/CFT compliance.

2.1.1. Board of Directors

- Approving, enforcing internal AML/CFT policy
- Establishing and approving the organizational structure, roles and responsibilities of AML/CFT of individual department/unit;
- Oversight on the risk management on AML/CFT.

2.1.2. President

- Ensuring that policies and procedures for AML/CFT Program are in line with changes and developments in products, services and information technology of the bank as well as development in modus for money laundering or terrorist financing.
- Ensuring that the implementation of AML & CFT Program is based on established policies and procedures.
- Ensuring that all employees, particularly employees of related work units and new employees have participated in ongoing training related to AML & CFT Program.
- Review and Approve all AML/CFT procedures.

2.1.3. Risk Management Committee

- Review and Support AML/CFT policy for the purpose of approval from Board of Directors.
- Periodically reviewing and updating AML/CFT policy.
- Monitoring AML/CFT related activities to implement AML/CFT policy.

2.1.4. Money Laundering Preventive Officer

Head – Compliance of the Bank shall be Money Laundering Preventive Officer who would have the necessary freedom to act on his own authority and shall report to President. Name, Designation, Address, Qualification, contact number, email address of the MLPO shall be informed to Financial Conduct Authority, for correspondence.

The Roles and Responsibilities of the MLPO shall be as follows:

- Submit Suspicious Transaction Report to FCA.
- Communicate Money Laundering Prevention to all staff periodically.
- To ensure laid down procedures on AML/CDD are followed in all units.
- To perform activities as required under Money Laundering Act, 2010, rules, directive issued by concerned authority.
- To develop and implement effective AML/CDD procedures for internal use.
- Ensure good coordination between operations and top management.
- To ensure timely reporting and maintenance of records of transactions exceeding threshold limit set by regulators.
- To carry out training to all staff on AML/CDD
- Report quarterly to BOD through President/Risk Management Committee on the compliance of AML/CFT Act/Rules/Directives issued by the FCA. Such report shall be submitted to FCA on half yearly basis.

2.1.5. AML/CFT officer

Designated officer at Compliance Department and Operation in charge of the various units shall act as AML/CFT (Anti Money Laundering / Counter Financing of Terrorism) Officer.

The major responsibilities of AML/CFT Officers will be as follows:

- To ensure compliance to Money laundering Prevention Act, 2010 along with internal AML Policy and AML/CDD procedures.
- To authenticate Know Your Customer (KYC) as required under AML/KYC procedures.
- To maintain record of Know Your Customer information as prescribed under AML/CDD procedure.
- To maintain record of transactions exceeding threshold limit and to file Transaction Threshold Report on fortnightly basis to Compliance Department.
- To ensure all staff of the branch have carried our in-house training on AML/CFT at least once every year.
- To file suspicious transactions report to Compliance Department of the transactions which donot match with general financial conditions of the customer.
- To keep customer's information confidential at all time.

3. Know Your Customer / Employee

Know your customer (KYC) is the process of business verifying the identity of its clients. The terms is used to refer to the Bank regulation which governs these activities. Banks are

increasingly demanding that customers provide detailed anti-corruption due diligence information, to verify their probity and integrity. Know your customer policies are becoming much more important globally to prevent identity theft, financial fraud, money laundering and terrorist financing. EmerioBanque shall not engage in business relationship for which customer identification and KYC is not performed.

3.1. Purpose of KYC

3.1.1. To establish procedures to verify the identification of individuals or corporate or other institutional accounts.
3.1.2. To detect suspicious transactions.
3.1.3. To establish process and procedures to monitor high value and suspicious transactions.
3.1.4. Establish systems for conducting due diligence and reporting of such activities.

3.2. Mechanisms Deployed for KYC

The Bank shall use various mechanisms for Customer Due Diligence / Know Your Customer. These activities shall be carried out at the time of account opening for all the type of accounts and services provided by EmerioBanque. Bank shall deploy all or the combination of any of the below mechanisms for KYC / CDD.

1. Customer Identification and Profiling
2. Risk Assessment
3. Documentary Evidence
4. Verification of Documents as per Original
5. Identification of Beneficial Owner
6. Politically Exposed Person (PEP) verification.
7. Restriction on Account Opening.

3.3. Know Your Employee

EmerioBanque shall have procedures in place that provide reasonable assurance of the identity, honesty and integrity of prospective and existing employees. These processes are being enhanced within the timeframes as per the FCA directives.

4. Suspicious and Large Value Transaction

This section of the document is intended to highlight about suspicious and large value transactions. The Bank will refuse any transaction where based on explanation offered by the customer of other information, reasonable grounds exists to suspect that the funds may not be from a legitimate source or are to be sued for an illegal activity such as terrorism, human trafficking etc. The bank shall use reasonable judgment in determining the suspicious transactions.

The understanding of customer's identity vis-à-vis his stated norms of dealings, services, etc would also have a bearing on transactions before they are viewed as suspicious transactions hence cautious approach in the process is very essential. Under no circumstances, bank will alert a customer about his transactions considered suspicious or that reporting is underway. The Bank will make prompt report of suspicious transactions, or proposed transactions to FCA through MLPO.

4.1. Transactions of Suspicious or Large Value in Nature

For identification of suspicious transactions, the Bank shall take precautions which would be exercised by a person of normal prudence. Some of the indications of suspicious transaction shall be:

4.1.1. Involvement of funds for illegal activity.
4.1.2. Intending to hide or disguise assets derived from illegal activities.
4.1.3. Intention to evade AML guidelines.
4.1.4. Customer has no business or apparent lawful purpose and has no linkage with such business.

4.2. General Characteristics of Suspicious and large Value Transactions

4.2.1. Transactions having unclear economical and business target.
4.2.2. Transactions conducted in relatively large amount cash and/or conducted repeatedly and unnaturally.
4.2.3. Transaction conducted differently from that of usually and normally conducted by the relevant customer.
4.2.4. Huge, complex and unusual transaction.

4.3. Elements of Suspicious and Large Value Transactions

4.3.1. Transaction deviating from:

4.3.1.1. the profile;
4.3.1.2. the characteristics; or
4.3.1.3. the usual transaction pattern of the relevant customer

4.3.2. Transaction suspected to have been conducted with the purpose of evading the reporting that must be conducted by the relevant reporting authority.
4.3.3. Financial transaction conducted using fund alleged to be attributable to predicate offences.

4.4. Detection of Suspicious and Large Value Transactions

There are different indicators to detect suspicious transactions. Detection of suspicious transactions for the purpose of preventing money laundering and controlling terrorist financing, this document has been made and issued exercising the power conferred by the Sanctions and Anti-Money Laundering Act 2018.

Based on this the bank shall use the below information for detection suspicious and large value transactions:

4.4.1. Individual Account's History

i. Threshold based detection

ii. Situation / Activity based detection

4.4.2. Transaction information from other accounts in peer group.

4.5. Terrorist Financing

Terrorist Financing provides funds for terrorist activity. The main objective of terrorist activity is to cause substantial property or human damage; or seriously interfering with or disrupting essential services, facilities or systems.

There are two main sources of terrorist financing – financial support from countries, organizations or individuals, and revenue-generating activities that may include criminal activities. The second source, revenue generating activities that may include criminal activities. The second source, revenue generating activities, may involve drug trafficking, human smuggling, theft, robbery and fraud to generate money. Funds raised to finance terrorism usually have to be laundered and this anti-money laundering processes in banks and other reporting industries are important in the identification and tracking of terrorist financing activities.

Bank shall build measures to monitor, identify and report such funds received or sent using the banks system. EmerioBanque shall take caution while doing transaction, account opening or carrying banking activities if in any circumstances the name of any banned organization or individual (involved in terrorist activities) appears as payee/endorsee/applicant and report such transaction as and when detected.

The Bank shall endeavor to get the list of such organization / individuals to the best possible means or mechanisms.

5. Correspondent and Shell Banks

EmerioBanque shall implement risk based due diligence procedures that include, but are not limited to, the following – understanding the nature of the correspondent's business, its license to operate, the quality of its management, ownership and effective control, its AML Policies, external oversight and prudential supervision including its AML/CFT regime.

Additionally, ongoing due diligence of correspondent accounts shall be performed on a regular basis or when circumstances change. Bank policies also ensure that we do not offer 'payable through accounts'. All correspondent banking relationships are approved by senior management of the bank.

5.2. Shell Bank

EmerioBanque shall not conduct business with shell bank. Our policies and procedures shall prohibit offering services to shell banks.

6. Account and Transaction Monitoring

The process (automated or manual) of monitoring transactions after the execution to identify unusual transactions, including monitoring single transactions as well as transaction flows, for subsequent review and, where appropriate, report to the authorities. The purpose of transaction monitoring is to provide ongoing identification of suspicious activity from customer transaction data.

Bank shall review the customer accounts on the basis of:

a. Account / Transaction monitoring and
b. Review of Account and Revision of Risk Level

6.1. Account / Transaction Monitoring

Money Laundering risk and CDD does not end after a customer has opened an account. To satisfy regulatory requirements and expectations as well as to protect the Bank, the respective employees must perform ongoing monitoring of our customer accounts. Employees must ensure that CSS documents, date or information retained are kept up-to-date and that assessment of AML Risk for the customer is appropriate. Bank shall deploy the below mechanisms for ongoing account monitoring. Bank shall do the ongoing monitoring of accounts based on:

- Threshold breach for all accounts and services
- Case logged by AML system
- Change of Account name
- Change of Shareholders
- Change of Signatories
- Change of Directors
- Activation of Dormant / Where About Unknown (WAUN) Accounts
- Account's transaction reported as suspicious
- It is apparent that the customer has become a PEP
- Customer name has been alerted through public media, regulatory authority as investigation, Newspapers, Public media, Home Ministry, UN Sanction List, INTERPOL, Financial Information Unit, Tax Office, Tax, Revenue Investigation, etc.

6.2. Account Review and Revision of Risk Level

Ongoing review of accounts is the process where the bank shall review all its accounts based on risk grading. For the purpose of account review is to check the risk level assigned. For this the bank, shall review the risk level of Level 2 A/Cs (Medium Risk Accounts) accounts in every 2 years and review of Level 3 A/Cs (High Risk Accounts) Accounts in every 1 year. After carrying out review of L2 / L3 Accounts, the risk level shall be reduced to lower risk on the following conditions:

- In case of L2 accounts, cumulative balance is less than prescribed threshold for both personal and non-personal accounts for the last 2 years.
- Signatories/Directors/Head of the organization /Shareholders/Beneficial Owners are no longer PEP
- Resident / Operating Address is no longer under High Risk Countries.
- Nature of business no longer falls under High Risk Business.

Joint approval of respective Segment Business Heads and Head Compliance shall be obtained for lowering of risk in all accounts.

7. Reporting Related to AML/CFT

When detecting suspicious transactions, or having the reasonable grounds to suspect the account transaction has derived from illegal activity or in relation with money laundering, Compliance Department must report to FCA under the confidential mode.

Bank shall also generate TTR (Threshold Transaction Report) and other reports related to AML/CFT.

8. Retention of Records

In terms of the operating procedures of the Bank, records such as Account Opening Forms, vouchers, ledgers, registers, etc., pertaining to Banking Transactions for specified periods are required to be maintained.

To assist the authorities on investigations of cases of suspicious money laundering, it is essential that evidence of customer identification, address, transaction details are retained by the bank as mandated by the regulators. Such records must be archived in a secure area under the custody of a dedicated custodian. Access to such records must be made available only with due approval from Head Compliance.

- Records of every transaction undertaken for / by a customer must be retained for 7 years.
- Account Opening / Closing forms / Internet Banking requests of the customers must be retained for 7 years from the date of closure.
- Documentary evidence of any action taken in response to internal and external reports of suspicious transactions must be retained for 7 years.
- Where it is known that an investigation is ongoing the relevant records must be retained until the authorities inform the Bank otherwise.

9. Policy Compliance

9.1. Employee Training Program

Training shall be provided to business units that offer products and services that are subject to the legislative requirements. Staff involved in customer facing areas, remittance, SWIFT etc., of the bank shall receive periodic training and reminders on the detection and reporting process for suspicious activities. Communications of changes to AML/CFT legislation or any emerging risks are communicated to the relevant staff.

In addition to the above, Human Resources Department shall make sure that the training on ALM/CDD will also be provided to all staff of EmerioBanque using internal or external resources and as and when there are changes in AML/CDD Policy/Procedures or there are new developments in the AML trends worldwide.

9.2. Amendment to the Policy

Financial Conduct Authority may issue the related circular / directives from time to time and the KYC/AML/CFT acts and laws of the country shall form integral parts of this policy. If any section / sub-section / clause of this policy contradicts with any laws, FCA directives or circulars; the latter shall be valid to the extent of contradiction.

This policy is subject to review at least annually or as required for updates in the terms or any clause of the policy. There shall be separate AML/KYC procedures formulated by the Bank.

9.3. Compliance measurement

MLPO or the designated officer will verify compliance to this policy through various methods, using various tool, reports, internal and external audits and feedback to the policy owner. Bank auditors and internal compliance departments shall conduct programs of audits and compliance testing of this policy and operational procedures applicable to AML. The frequency of the audits and compliance tests are determined through risk-based approach, where higher risks to EmerioBanque are audited and tested more frequently. The audit and compliance programs shall be approved by senior management.

9.4. Exceptions

Any exception to the policy must be acknowledge by MLPO and approved by the Bank Management.

9.5. Non-Compliance

An employee found to have violated this procedure may be subject to disciplinary action, as per the provisions in the prevailing EmerioBanque Employee Bylaw.