ALPHA BANK

Synopsis of the ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM (AML/CFT) POLICY
(As approved by the Bank's Board of Directors on 28.01.2021)

GROUP POLICY FRAMEWORK

The legalisation of proceeds of criminal activities or "Money Laundering" (hereinafter "ML") refers to all actions and activities intended to conceal or disguise the illegal source, or acquisition, possession or use of property knowing that such property is derived from criminal activity or from an act of participation in such an activity.

The financing of terrorism (hereinafter "FT") is the provision or collection of funds, directly or indirectly, with the intention that they will be used or in the knowledge that they are to be used, in order to carry out any of the terrorist offences.

The solvency, the integrity and the reputation of the Bank and of the Group, as well as the reliability of the financial system in general, may suffer greatly as a result of the efforts made by criminals to conceal the source of the proceeds of criminal activities or to channel funds to terrorist activities.

The Bank, identifying the risks arising from ML and FT activities/actions and their potential consequences, as well as the importance of combating financial crime, the regulatory framework in force and taking also into account the provisions of the recommendations of the Financial Action Task Force (F.A.T.F.), applies at Group level the present AML/CFT Policy, which has been approved by the Bank's Board of Directors. The Policy is fully complied with the provisions of the EU Directive 2015/849, as amendment by the EU Directive 2018/843.

The Group Companies and Branches of the Bank operating in Greece and abroad shall implement the current AML/CFT Policy by laying down specialised procedures and installing appropriate IT systems.

More specifically:

The Procedures:

- Are adapted to the nature of the business activities of each Group Company and comply with the applicable local regulatory framework.
- Are assessed periodically and are revised when deficiencies are identified or when the need to be updated arises.
- Are approved by the Board of Directors or the Executive Management of the Group Company and must be communicated to the Company's employees, to whom duties and responsibilities are clearly allocated.

The IT Systems:

- Are appropriate to provide timely and reliable information for the monitoring of the clientele and the transactions, on the basis, among others, of the lists issued by the various Authorities of persons or entities subject to sanctions.
- Allow continuous monitoring and detection of transactions or activities which may be associated with ML or FT, by means of defined parameters (such as indicative typology of transactions, customer's financial/transactional profile, expected account activity etc.).

February 2021

The key components of the AML/CFT Policy are the following:

- Responsibilities of the AML/CFT Officer
- Risk Assessment
- Customer Management
- Continuous Monitoring of Accounts and Transactions
- Reporting of Unusual/Suspicious Transactions
- Compliance with other Obligations prescribed in the Regulatory Framework.

RESPONSIBILITIES OF THE AML/CFT OFFICER

The Group Manager of Compliance is appointed as the responsible AML/CFT Officer for ensuring that the Group's obligations, as a whole, regarding the prevention of the use of the Financial System for money laundering and terrorist financing, are met.

Each Group Company and each Branch of the Bank abroad shall appoint an AML/CFT Officer and an alternate thereof. The AML/CFT Officer shall be responsible for ensuring the proper and adequate implementation of the AML/CFT Policy.

An AML/CFT Special Service shall be established in the Compliance Unit of each Group Company. The Board of Directors of the Group Company shall ensure the independence of the AML/CFT Special Service.

RISK ASSESSMENT

Taking into account that the risk of ML and FT varies among different cases, Group Companies apply a comprehensive Risk-Based Approach, which:

- Entails evidence-based decision-making so that emphasis is given on the ML/FT risks.
- Is based on the need to identify, analyze, assess and mitigate risks.
- Is revised annually or earlier, if deemed necessary.

Therefore, the Group Companies adopt appropriate measures to identify and assess the ML/FT risks, taking into account risk factors among which those related to customers, countries or geographical areas, products, services, transactions or banking service channels.

Additionally, Group Companies implement policies, controls and procedures to effectively mitigate and manage the relative risks identified at both Company and country level.

CUSTOMER MANAGEMENT

A fundamental component of the customer acceptance and cooperation policy is the "Know Your Customer" (KYC) Principle which is the basis of all AML/CFT procedures and provides for the collection and retention of adequate information about the customer with a view to:

- Their identification and verification of their identity; and
- The assessment of their overall profile.

The application of the "Know Your Customer" principle and the assessment of information collected about the customer allows the profiling of the customer's risk and their classification in risk categories, based on specific criteria.

Customers are categorized depending on the risk of money laundering and terrorist financing in at least four risk categories, as follows:

- Unacceptable Customers
- High-Risk Customers
- Medium -Risk Customers
- Low-Risk Customers

CONTINUOUS MONITORING OF ACCOUNTS AND TRANSACTIONS

It is achieved by compliance with the procedures and, mainly, using appropriate IT systems and applications.

The purpose of continuously monitoring accounts and transactions is to identify unusual or suspicious transactions which, due to their nature may be related to ML/FT.

REPORTING SUSPICIOUS/UNUSUAL TRANSACTIONS

Upon detection of unusual or suspicious transactions that are not justifiable based on the existing information, said transactions shall be reported to the competent FIU.

The report shall be made as per the provisions of the local regulatory framework and the internal procedures of the Group Company.

COMPLIANCE WITH OTHER OBLIGATIONS UNDER THE REGULATORY FRAMEWORK

Training

Compliance Division provides on a regular basis to the employees complete and up-to-date training programmes that respond to ever-changing conditions.

Performance by third parties

Under specific conditions, it may be possible to assign intermediate or third parties with carrying out the procedure for Customer identification and verification. In any case, the final responsibility for customer identification and verification is borne by the Group Company that relies on a third party.

Record Retention

All details and information collected are kept in printed or electronic form for a period of five years after the end of the business relationship with the Customer or the date of the occasional transaction. Upon expiry of that period, the Group Company shall delete the personal data, unless their keeping for longer periods, which may not exceed ten years, is permitted or reasonably required by any other law or regulation.

Assessment of the System for the prevention of money laundering and terrorist financing

The Internal Audit Unit of the Group Company carries out specialised controls to identify, assess, monitor and manage the risk of money laundering and terrorist financing.