attica bank

Anti-Money Laundering (AML) / Combating the Financing of Terrorism (CFT) and Know your Customer (KYC) Policy

attica bank

Table of Contents

1. Introduction

ATTICA BANK SA is committed to applying the highest level of standards in order to manage Anti-Money Laundering (AML) and Counter Terrorist Financing (CTF) risks and ensure transparency in its business activities.
This Policy is fundamental to manage compliance with relevant and applicable laws and regulations relating to Money Laundering and Terrorist Financing by applying appropriate Customer Due Diligence (CDD) and Enhanced Due Diligence procedures in the context of Know Your Customer. In addition, this Policy sets the framework for assessing and monitoring customer transactions which is also fundamental in ensuring AML and CFT risks are adequately managed.
This Policy is subject to review on an annual basis. Updates are recommended by the AMLO and / or the Chief Compliance Officer, reviewed by the Audit Committee and approved by the Board of Directors.
The controls defined within this Policy aim to protect the Bank by detecting, preventing and deterring those attempting to circumvent AML & CFT regulations by future engagement with the Bank.

1.1 Policy Objectives

The objectives of this Policy are to:
• Adhere to the AML & CFT regulatory framework
• Mitigate potential compliance, regulatory and reputational risks associated with infringements of AML & CFT regulations
• Set guidelines and serve as a point of reference to all Bank employees and officers on matters relating to money laundering, terrorist financing, customer due diligence, enhanced due diligence, and in assessing and monitoring customer transactions
• Protect the Bank's reputation.
The Policy defines the minimum legal, regulatory and internal requirements to be complied with for managing AML & CFT risks. The Bank will ensure that it does not establish relationships or transact with individuals and entities ("persons") or governments that attempt to circumvent AML & CFT regulations.

1.2 Scope

This Policy applies to all employees of ATTICA BANK SA, including Head office and branches.

1.3 Terms and Definitions

Money Laundering
Money Laundering involves taking criminal proceeds and disguising their illegal source in anticipation of ultimately using the criminal proceeds to perform legal and illegal activities. (see Crimes according the Art.4 – Law 4557/2018 in APPENDIX II).
According to article 2, par.2 of Law 4557/2018, the following conduct, when committed intentionally, shall be regarded as money laundering:

(a) the conversion or transfer of property, knowing that such property is derived from criminal activity or from an act of participation in such activity, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such an activity to evade the legal consequences of that person's action;
(b) the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of, property, knowing that such property is derived from criminal activity or from an act of participation in such an activity;

(c) the acquisition, possession or use of property, knowing, at the time of receipt, that such property was derived from criminal activity or from an act of participation in such an activity;
(d) participation in, association to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the actions referred to in points (a), (b) and (c).

4. Money laundering shall be regarded as such even where the activities which generated the property to be laundered were carried out in the territory of another Member State or in that of a third country.

Terrorist Financing

"Terrorist financing' means the provision or collection of funds, by any means, directly or indirectly, with the intention that they be used or in the knowledge that they are to be used, in full or in part, in order to finance an act of terrorism.

Terrorist financiers can either knowingly or unknowingly provide funds toward terrorist activities, often with funds generated from legitimate sources as well as those accrued from illegal criminal activity.

Terrorists use techniques similar to money laundering to evade the attention of authorities and to protect the identity of their sponsors and ultimate beneficiaries. The challenge for financial institutions is identifying where transactions, particularly from legitimate sources, may be linked to parties known to fund terrorism as the financial destination is not always prevalent at the time of the transaction.

Know Your Customer, Customer Due Diligence, Enhanced Due Diligence

Know Your Customer refers to identifying the customer, the ultimate beneficial owner, understanding the nature of their business, the source of income, the source of wealth and the source of funds.

Customer Due Diligence is the act of gathering information about the customer's activities which enables the Bank to develop a risk profile which can be reliable in identifying unusual or suspicious activity.

Furthermore, understanding the parties associated with a customer can help provide the Bank with a more detailed view of the Money Laundering/Terrorist Financing risks associated with the customer.

Enhanced Due Diligence is the procedure implemented for the identification and monitoring of customers who pose a higher risk of being involved in acts related to money laundering and/or financing terrorism.

Source of Income

Source of income is the occupation/ business from which a customer may receive regular and recurring compensation from all sources. Depending on the customers' situation, it may include income received from:

a) Employment (salary income)
b) Self-employment
c) Business or profession
d) Recurring income from property
e) Pension entitlements
f) Any other recurring sources

Source of Funds

The source of funds refers to the origin of the particular funds or other assets, which flow from/ through a financial institution to the account of the customer, the amounts being invested, deposited, or wired as part of the business relationship. Normally, this is related to the value of "flow" of a transaction between the customer and the financial institution.

Source of Wealth

The source of wealth refers to the activity or situation that has generated the customer's total wealth or net worth. For example, inheritance, sale of asset(s), long-term investments or business ownership. The value of the customers' "wealth" is generally "static" in nature and does not vary on a regular basis.

Global and Internal Lists

Both international and local/ internal list, such as the OFAC and SDN Lists, that the Bank uses to screen its customer and transactions against (please refer to ATTICA BANK SA Customer Acceptance Policy).

1.4 Risk Appetite

It is the Policy of ATTICA BANK SA to fully comply with all relevant and applicable AML & CFT regulations.

The Bank has zero tolerance for breaches of AML & CFT laws or regulations and prohibits any activity that serves the purpose of permitting any government, entity or person to breach or circumvent them.
The Bank will adopt a Risk Based Approach to manage compliance with all relevant and applicable AML & CFT regulations.
The Bank's Board of Directors is accountable for setting the Bank's risk appetite and ensuring a strong compliance culture across the Bank.
The present policy together with the Customer Acceptance Policy articulate the Bank's key risk appetite statements relevant to Regulatory Compliance and Financial Crime risks. On an annual basis or more frequently, if necessary, Compliance will review the risk appetite statements and provide recommendations on any amendments. These recommendations shall be reviewed by the Audit Committee and approved by the Board of Directors.

1.5 Adherence to this Policy

All the Units within the Bank must comply with the requirements outlined in this Policy. The Bank has adopted an effective controls framework to ensure compliance with this policy and respective procedures, law and regulations.

1.6 Policy Breaches and Circumvention

A Policy breach is defined as any instance where requirements set by this Policy have not been met.
The Bank maintains a position of zero tolerance on intentional breaches of law, regulation or compliance Policy. Employees are responsible for reporting any known breach, attempt to evade or intention to circumvent this Policy to Compliance. Violations of the AML Legal & Regulatory framework entail responsibilities (notwithstanding legal ones), for both, the physical person and the legal entity involved, as well as administrative fines as specified in articles 45 and 46 of Law 4557/2018 and the respective, implementing Acts of Bank of Greece.

1.7 Authorities/Regulators

The Bank of Greece is the authority responsible for supervising compliance with the legislative Framework on the prevention and suppression of money laundering and terrorist financing ("AML/ CFT – Framework") by the institutions falling under its supervisory Authority.
The Hellenic Financial Intelligence Unit - Anti-Money Laundering, Counter-Terrorist Financing and Source of Funds Investigation Authority ("The Commission"). The Commission is the national unit which aims at combating the legalization of proceeds from criminal activities and terrorist financing, assisting in security and sustainability of fiscal and financing stability. Its mission, is the collection, the investigation and the analysis of suspicious transactions reports that are forwarded to it by legal entities and natural persons, under special obligation, as well as other information that is related to the crimes of money laundering and terrorist financing.

1.8 Control and Maintenance of this Policy

Compliance function shall be the Controller of this Policy. All inquiries and requests relating to any of the matters specified in the Policy should be addressed to the DIRECTOR or his substitute.
As ATTICA BANK SA and its operations evolve, it is anticipated that existing policies may require amendment, and new policies will need to be introduced. The policy should be reviewed on an annual basis or more frequently, if required, to ensure it is kept up to date. All amendments, additions or deletions to the Policy should be properly documented and authorized/approved prior to implementation.
This Policy should be posted on ATTICA BANK SA's internal website. This Policy must not be copied or revealed to third parties without the written permission of the Money Laundering

Reporting Officer (MLRO) and Senior Management, (if required). Unauthorized sharing of this Policy (both hard copies and electronic copies) with individuals and entities outside ATTICA BANK SA is strictly prohibited. Violators of this Policy are liable to disciplinary action.

2. Policy Statement Key Principles

• ATTICA BANK SA applies a risk-based approach to conducting due diligence on new and existing customers including enhanced due diligence for customers presenting a high risk exposure (or with a high risk profile).
• ATTICA BANK SA enters into a relationship with a prospective customer only if the purpose of the relationship, identity of the customer and the Ultimate Beneficial Owner ("UBO") can be established, and ad hoc.
• ATTICA BANK SA establishes controls to ensure on-going update of customer profiling details and other related information in accordance with the customer risk rating on event driven basis.
• ATTICA BANK SA ensures appropriate screening controls are in place for customers, non-customers and applicable connected parties at on-boarding, periodically through the course of the relationship and ad hoc.
• ATTICA BANK SA shall implement appropriate monitoring controls of client accounts and transactions to detect unusual/suspicious transactions using adequate processes and systems.
• ATTICA BANK SA shall establish appropriate investigation escalation and reporting requirements to deal with unusual/suspicious activities;
• ATTICA BANK SA identifies and avoids transactions that could expose the Bank an any of the transaction participants, including customers, employees and counterparties, to the risk of violation of the applicable regulatory framework.
• ATTICA BANK SA ensures that appropriate processes shall be in place to support requests from regulators, government agencies and law enforcement bodies in identifying and combatting Money Laundering/Terrorist Financing risks.
• ATTICA BANK SA shall establish learning and awareness training programs for all employees on identification, mitigation and reporting of AML & CFT risks.

3. AML & CFT Governance and Accountability

ATTICA shall establish the three Lines of Defence model to ensure a clear delineation of responsibilities between day-to-day operations, monitoring and oversight, as well as independent assurance to achieve effective governance.

The established three lines of defence model are described below:

1st Line of Defence

The Bank's Units act as the 1st Line of Defence and are responsible for identifying, managing and mitigating risks as part of the day-to-day operations.
The Units are responsible for ensuring that a risk and control environment is established as part of day-to-day operations. The business should be adequately skilled to identify Compliance risks and establish controls for managing those identified risks. Active Compliance Risk Management and periodic reporting is crucial for quick identification and response, and allows ATTICA to have a strategic advantage on competitors.

2nd Line of Defence

Compliance Function acts as the 2nd Line of Defence and provides advice,support, monitoring and challenges the 1st Line of Defence to ensure risks are identified and managed.
Specifically, Compliance as the 2nd Line of Defence is responsible for:

- Notifying and guiding the 1st Line of Defence on emerging issues and changing applicable regulatory framework.
- Advising, supporting and challenging the 1st Line of Defence on business related risks.
- Assisting management in developing processes and controls to identify and manage risks.
- Providing guidance and training on risk related rules, regulations and procedures.
- Monitoring the adequacy and effectiveness of controls.

3rd Line of Defence

The Internal Audit Division acts as the 3rd Line of Defence. Its role is to provide independent, objective assurance and consulting activities designed to add value and improve the Bank's operations. The Internal Audit Division helps the Bank to accomplish its objectives by bringing in a systemic, disciplined approach to evaluate and improve the effectiveness of risk management controls. It also independently reviews the effectiveness of the 1st and 2nd Lines of Defence.

3.1 Roles and Responsibilities

Board of Directors

The BoD has the principal responsibility for establishing appropriate systems and controls to ensure adherence with its stated Risk Appetite and regulatory requirements.

The BoD has the following responsibilities towards Compliance Function:

• Approve the establishment of a permanent Compliance Function

• Oversee the management of the Compliance Function through the Audit Committee.

The Bank of Greece requires that a Greek firm's senior management have responsibility to ensure that the firm's control processes and procedures are appropriately designed and implemented and are effectively operated to reduce the risk of the firm being used in connection with money laundering or terrorist financing. Senior management must be fully engaged in the AML/CTF decision making processes and must take ownership of the risk-based approach, since they will be held accountable if the approach is inadequate.

Senior management, in the context of an effective risk management strategy according to the provisions of BOG GA 2577/2006, shall:

• Adopt an AML/CTF policy, which shall be recorded, documented and approved by the firm's Board of Directors; to this end, each firm' shall have an Anti-Money Laundering Reporting Officer (MLRO), a relevant unit, the resources required and adequate staff;

• Specify the role, responsibility and duties of the AMLO and the unit he/she heads;

• The MLRO shall be appointed by the firm's Board of Directors based on his/her morality, integrity, status, background, experience in the relevant field and familiarity with a firm's operations;

• If the MLRO is unavailable, he/she shall be replaced by an alternate appointed together with him/her; their data shall be communicated to the Bank of Greece within ten days of commencing their roles;

• Allocate clear responsibilities and duties to the persons and units involved in the firm's transactions and operations, to ensure effective implementation of AML/CFT policy, procedures and controls and achieve compliance with the legal and regulatory framework

•Take appropriate measures so that its management and staff are informed about the provisions of the legal framework as well as the firm's policies and procedures specifying them, and ensure their participation in specialised AML/ CFT training courses;

• Ensure the evaluation of the customer's overall business portfolio maintained with the firm and, possibly, with other companies in its group, in order to confirm that the transaction examined as suspicious or unusual is consistent and compatible with such portfolio(s); and

• Take any appropriate measure, including refusing to execute the transaction or terminating the business relationship with the customer and the beneficial owner, in the event that identification and verification conditions have not been fulfilled, Customer Due Diligence measures have not been observed; or reports on the customer in question have been repeatedly submitted to the Commission.

Anti-Money Laundering Officer (AMLO)

According to Law 4557/2018 (Art.38) each Credit Institution owes to assign a Managerial Executive (and deputy), to whom other managerial executives and employees, will report each transaction that they consider suspicious of legalization of income from criminal activities and each fact, for which they are informed, during the exercise of their duties, and which could constitute indication of criminal activity.

Under this respective the Bank shall appoint an Anti-Money Laundering Officer who will refer to the Chief Compliance Officer. The Money Laundering Reporting Officer (MLRO) shall have the responsibility for the overall direction of the Bank's AML & CFT Policy and procedures.

The MLRO reports to the Audit Committee and the Chief Executive Officer.

The Authorized Executive Employee has at minimum the following duties (according to the provisions of Governor's Act 2577/2006):

• Assisting the Bank in its responsibility for complying with all relevant AML & CFT regulations,including the provision of advice on money laundering & terrorist financing issues

• Establishing guidelines to detect money laundering operations and combat financing terrorist and illicit organizations

• Identifying and assessing AML & CFT risks associated with the Bank's business activities, including in relation to the development of new products, the proposed establishment of new business or customer relationships, or material changes in the nature of such relationships

• In case the Bank is based in third parties about the validation and the verification of Customers' IDs, evaluates the framework for the collaboration with Correspondent Banks, and evaluates the mechanisms, the procedures and the AML/FCM software that the third parties are using.

• Coordinating and liaising with Senior Management in planning how money laundering and terrorist financing deterrence should be organized and operated

• Undertake investigations into potential breaches, regulatory issues in conjunction with otherstakeholders as appropriate

Establish and maintain an appropriate AML & CFT training programme and adequate awareness arrangements across the bank

• Respond promptly to any request for information made by Competent Authorities on money laundering and financing of terrorist matters

• Establish and manage communication of applicable rules and regulations relating to AML & CFT

• Act as the subject matter expert and point of reference to address related queries on AML & CFT across the respective legal entity

• Manage periodic submission of appropriate reporting to Competent Authorities on Money Laundering matters

• Identify and report suspicious transactions to the Hellenic FIU and the competent BoG Division (AML Bank of Greece)

• Review AML & CTF regulations and procedures and the extent of the Bank's compliance with the implementation, propose actions required for their update and development, develop periodic reports in this regard and submit them to the Senior Management

• Cooperate with the Hellenic FIU and the competent BoG Division (AML Bank of Greece) by providing data and information required for undertaking their tasks.

• Act as the main liaison officer with the Central Bank, the Units and branch network to ensure timely and effective reporting of suspicious transactions, as defined in regulations issued by the local competent authorities, and give guidance on KYC activities to be carried out by the Branches and Units

• Represent the Bank when dealing with Regulatory Authorities in relation to AML & CFT and other Regulatory Compliance matters and the reporting thereof

• Act as the central point for the receipt of reports on reportable transactions and/or activities from the Units and Branches, the recording and investigation thereof and escalation of reports deemed to require further investigation by the authorities

• Evaluates the Internal Audit Reports and asks for corrective actions in AML/ CFT issues.

• In case of recommendations identified and issued from Bank of Greece asks for corrective actions and the enhancement and / or implementation of the new procedures.

• The AMLO must have a level of authority and independence within the firm and access to resources and information sufficient to enable him/her to carry out the AMLO's responsibilities.

Furthermorer he is required to ensure that ATTICA complies with all applicable AML & CFT laws and regulations, rules, policies and procedures, having the responsibility to:

- Oversee the implementation of the Bank's Compliance Framework, functioning as an independent and objective body that reviews and evaluates compliance issues/concerns
- Ensure that the Bank is fully aware of and complies with all relevant AML & CFT regulations
- as well as local and international leading practices that fosters the development of a compliance culture

- Ensure that the Audit Committee is kept informed of all material compliance issues and problems
- Ensure that the Bank's Senior Management is informed of all critical Compliance plans and initiatives
- Provide advisory services (and training where appropriate) to Units to achieve compliance
- with all Compliance related policies, procedures, laws, rules, regulations, systems and plans
- Liaise with Internal Audit Function on Compliance related matters
- Manage the Compliance Function to ensure that it is properly established and effective
- including assessment of staff to ensure that they have the skills and experience to fulfil their responsibilities
- Ensure that ATTICA Compliance Function maintains an appropriate Compliance Framework, composing of clear definitions of roles, responsibilities and reporting lines and adequate policies and procedures covering AML & CFT
- Ensure that violations of the Policy or any relevant regulations, procedure or process are appropriately identified and escalated
- Monitor the complete rollout of all AML & CFT mandatory training taking a leading role in the delivery of face-to-face training, particularly to the BoD and Senior Management
- Take a leading role in establishing and maintaining all key relationships with Regulatory Authorities, external auditors, correspondent banks and other key external stakeholders
- Ensure the implementation and maintenance of complete, accurate and relevant reporting process.

4. RISK BASED APPROACH

The Bank adopts a risk-based approach to manage compliance with all relevant and applicable AML & CFT laws and regulations. The Bank has established risk-based Customer Due Diligence, Identification, Verification and Know Your Customer (KYC) procedures, including Enhanced Due Diligence (EDD) for those customers presenting higher risk, such as Politically Exposed Persons (PEPs) and Corresponding Banking relationships and applicable ongoing monitoring procedures.
Customers are categorized as Low, Medium and High based on the AML & CFT risk they pose. Assessment is performed as per the AML & CFT Risk Assessment Methodology, on the basis of the annexes I and II of Law 4557/2018 (see Appendix I) and the relevant guidelines of EBA, as analyzed in the relevant procedures of the bank.
Due diligence and the extent of the measures to apply depend on the level of risk, which inter alia is defined by:
I. the professional and the financial size of the customer,
II. The purpose of the business relationship,
III. The type, frequency, and the value of transactions,
IV. The expected origin and destination of funds,
It must be proved to the competent authorities that the extent of the measures must be proportionate to the risks of money laundering offenses and financing of terrorism and that they apply these measures with consistency and effectiveness.

4.1 Customer Due Diligence (CDD)

Identifying the customer, the ultimate beneficial owner, understanding the nature of their business and bot the source of income, source of wealth and source of funds is a requirement for effective AML & CFT compliance. The CDD process enables the Bank to develop a risk profile for the customer in an effort to enable effective AML & CFT risk management.
CDD comprises of:
• Customer Identification & Verification
• Know Your Customer
• Enhanced Due Diligence for higher risk customers
• On-going Due Diligence
• Know Your Business (KYB) and Know Your Customer's Customer (KYCC) (for non-individual customers).

ATTICA shall take into consideration the total portfolio of the client with the bank and other companies of the Group, to the extent applicable, when evaluating a transaction, in order to examine the suitability of the transaction to the economic profile of the client. Additionally, at the establishment of the relationship the Bank will verify the annual income of the client by asking a tax clearance certificate.
Customer Due Diligence (CDD) enables the Bank to manage its money laundering and financing terrorism risk exposure through:

- Identification of customers that fall within the Bank's risk appetite
- Building accurate and reliable customer risk profiles facilitating risk-based decisions
- Application of risk-based customer monitoring based on objective risk rating methodologies
- Identification of unusual or suspicious transactions based on the Bank's knowledge of the customer and their anticipated activity.

ATTICA shall develop its CDD controls whilst maintaining a risk-based approach. Units must ensure that CDD is performed prior to establishing a relationship, periodically throughout the term of the relationship and in response to trigger events.
The Bank will not deal with any customers where KYC standards and due diligence cannot be applied or ultimate beneficial owner cannot be identified.

4.2 Customer Identification and Verification

Identification and verification of a customer (and Connected Parties as in the case of PEPs) provides the Bank with an understanding of whom it is doing business with. This is a 2-step process:
a) **Identification** – the process of identifying whom the prospective customer is and the Connected Parties linked to it.
b) **Verification** – the process of confirming the identification information gathered against documents, data or information obtained from reliable or independent sources.
ATTICA shall have processes and controls in place to identify as a minimum the following data points for each customer type:
• Name of customer
• Legal existence of customer
• Residence/Establishment
• TAX ID
• Name of those exercising control over the customer
• Name of those exercising ownership of the customer (for non-individuals, i.e. ultimate beneficial owners).
A detailed list of mandatory data points required to be captured in the Bank's system is included in the KYC Procedure document.
All reasonable steps should be taken to establish the true and full identity of all parties involved in a single relationship. The Bank will not enter into a relationship with any individual and entity
• Whose identity cannot be confirmed
• Who do not provide all the required information
• Who have provided false information
• Who have provided information with significant inconsistencies.

4.3 Know Your Customer (KYC)

Gathering information about the customer's activities enables the Bank to develop a risk profile which can be reliable in identifying unusual or suspicious activity.
Furthermore, understanding the parties associated with a customer can help provide the Bank with a more detailed view of the AML & CFT risks associated with the customer.

As part of the KYC process, Units have processes in place to obtain information on the following:
Purpose of the Relationship –
The Bank must document the intended purpose of the relationship and assess if the purpose aligns to the products and services being used by the customer.

Source of Income –
Units must establish the customer's form of employment/ employer and the customer's level of income.
Source of Funds –
The source of the funds used by the customer to fund their account must be identified.
Source of Wealth –
Units must document how the customer has generated their wealth. Understanding the source of wealth enables the bank to identify links to activities deemed outside of ATTICA's risk appetite.
Politically Exposed Persons (PEPs) –
Names of the customer, applicable connected parties,(husband, wife, children and their husband and wife, close partners, parents), shareholders and ultimate beneficial owners must be screened against PEP data to identify possible links to PEPs which may present a higher AML & CFT risk and require EDD review.
Watch List Screening –
Names of the customer and of the legal representatives/physical persons in case the customer is a legal entity, applicable connected parties (eg in the case of PEPs), shareholders and ultimate beneficial owners must be screened against internal and external lists to identify possible links to parties or activities deemed outside of ATTICA's risk appetite.

4.4 Enhanced Due Diligence (EDD)

Where information indicates a higher risk of financial crime (i.e. high risk customer as per the Bank's AML & CTF Risk Assessment Methodology), mitigating controls should be in place to manage the increased risk exposure. EDD, according to the provisions of the Decision of the Bank of Greece, numb. 281/17.3.2009 par. 4, if performed properly, can enable the Bank to manage and mitigate higher risks.
All customers identified as high risk must be subject to EDD. Reassessing of high risk customers and business relationships should take place on an annual basis.
For High Risk customers, EDD requirements apply in addition to the standard identification and verification requirements.
Indicatively, specific cases that must always be treated as high risk and subject to EDD include:

- Where the customer, or the customer's beneficial owner, is a PEP
- Correspondent relationship with a respondent Institution from a non-EU state
- Relationships with natural persons or legal entities established in high-risk for AML third countries, as defined by the EC that do not comply adequately with the FATF recommendations
- All complex and unusually large transactions, or unusual patterns of transactions, that have no obvious economic or lawful purpose.
- Customers or thirds parties with complex and/or non-transparent legal structures (e.g.
- Accounts of companies with bearer shares; Accounts of offshore companies and special purpose vehicles, "SPVs", Accounts of Trusts; Accounts of non-profit organisations)
- Non-face to face customer relationships
- Business relationships and transactions involving high risk of tax evasion.

<u>High risk categorization is distinguished</u> in at least:

- Accounts of Non-Resident customers
- Accounts of Politically Exposed Persons and their close relatives and collaborators
- Accounts of companies with anonymous shares when specific criteria are not fulfilled
- Accounts of off-shore companies and companies of special purpose vehicle
- Trusts, Holdings and Asset Management Companies
- Accounts of Unions & Foundations with non-profitable character
- Private Banking and Private Asset Management
- Portfolio Administration of Important Customers
- Cross-border relations of banking correspondence with third countries
- Countries that do NOT apply the FATF recommendations (see Appendix II)

<u>EDD measures include:</u>

- Increasing the quantity of information obtained for CDD purposes (including the customer's economic profile (tax certificate) against actual customer activity)

- Increasing the quality of information obtained for CDD purposes to confirm the customer's or beneficial owner's identity
- Verifying the customer's and the beneficial owner's identity on the basis of more than one reliable and independent source
- Identifying, and verifying the identity of, other shareholders who are not the customer's beneficial owner or any natural persons who have authority to operate an account or give instructions concerning the transfer of funds or the transfer of securities
- Obtaining more information about the customer and the nature and purpose of the business relationship to build a more complete customer profile, for example by carrying out open source or adverse media searches or commissioning a third party intelligence report
- Increasing the frequency of transaction monitoring
- Reviewing and, where necessary, updating information and documentation held more frequently.
- Where the risk associated with the relationship is high, the business relationship should be reviewed annually.
- Correspondent relationship with a respondent Institution from a non-EU state
- Relationships with natural persons or legal entities established in high-risk for AML third countries, as defined by the EC that do not comply adequately with the FATF recommendations
- All complex and unusually large transactions, or unusual patterns of transactions, that have no obvious economic or lawful purpose.
- Customers or thirds parties with complex and/or non-transparent legal structures (e.g. Accounts of companies with bearer shares; Accounts of offshore companies and special purpose vehicles, "SPVs", Accounts of Trusts; Accounts of non-profit organisations)
- Non-face to face customer relationships
- Business relationships and transactions involving high risk of tax evasion.
- Adverse information on the customer or its connected parties indicates links to criminal organisations or activity.

Compliance must be consulted to mitigate the risk of a transaction involving counterparties, products or services under sanctions /embargoes or potentially linked to other criminal activities.
On the other hand, Compliance should keep updated the personnel of the bank of published sanctions, embargoes and/or relevant guidelines to mitigate the risk of the bank being (indirectly) involved in situations generating compliance risk.

4.7 On-going Due Diligence

On or more of the following triggers can lead to an event or transaction driven review:
• New higher-risk products or services taken up by the customer
• Positive matches on PEP lists
• Transaction monitoring findings identifying material changes in account activity
• Suspicious Activity Reports raised
• Re-activation of dormant account
• Regulatory action/censure/request for information
• Adverse information identified
• Summons/Subpoena issued on the customer by law enforcement
• Change in country of operations or head office
• Change in nature of business which impacts risk rating
• Material change in ownership (i.e. new beneficial ownership or controlling parties)
• Changes to Group risk appetite or requirements defined within Policies
• Several changes to customers' address and ID.

On-going reviews must include:
• Updates to CDD and EDD information (as applicable). Reassessing of Low and Medium risk customers and business relationships should take place every three (3) years but for High risk should be updated annually.
• Obtaining valid documentation where existing documents have expired, as applicable

• Rescreening customer and connected party names against PEP data and AML lists
• Reviewing the customer's account activity against expected activity as documented within the customer profile
• Review of the customer's risk rating through the AML & CFT Risk Assessment Methodology.

4.8 Correspondent Banking

According to FATF "Correspondent banking is the provision of banking services by one bank (the "Correspondent bank") to another bank (the "Respondent bank")".
Correspondent accounts enable respondent banks to conduct business and provide services that they cannot offer directly (because of the lack of an international network). The correspondent bank processes/executes transactions for customers of the respondent. The correspondent bank generally does not have direct business relationships with the customers of the respondent bank, who may be individuals, corporations or financial services firms. Because of the structure of this activity and the limited available information regarding the nature or purposes of the underlying transactions, correspondent banks may be exposed to specific AML & CFT risks.
To address these risks, banks must undertake customer due diligence measures to gather sufficient information, to fully understand the nature of the respondent's business and correctly assess AML & CFT risks on an ongoing basis.
Factors that ATTICA, as correspondent bank, should consider include:
• The jurisdiction in which the respondent bank is located
• Take into account the country assessment reports of FATF, the International Monetary Fund and the World Bank, as well as other independent and reliable sources, to evaluate the adequacy of the AML/ CFT system in place in the correspondent institution's country of establishment

• The group to which the respondent bank belongs, and the jurisdictions in which subsidiaries and branches of the group may be located
• Information about the respondent bank's management and ownership (especially the presence of beneficial owners or PEPs), its reputation, its major business activities, its customers and their locations
• The purpose of the services provided to the respondent bank
• The respondent bank's business including target markets and customer base
• The condition and quality of banking regulation and supervision in the respondent's country (especially AML & CFT laws and regulations) including financial institution's regulatory status and history.
• The money-laundering prevention and detection policies and procedures of the respondent bank, including a description of the CDD applied by the respondent bank to its customers and how it meets internationally recognised standards and sufficiency to mitigate the risk presented based upon their products, customer base and jurisdiction
• The ability to obtain identity of any third-party entities that will be entitled to use the correspondent banking services.
• The potential use of the account by other respondent banks in a "nested" correspondent banking relationship.
• With respect to payable-through accounts, be satisfied that the correspondent institution has verified the identity and performed ongoing monitoring of the customers having direct access to accounts of the correspondent, and that it is able to provide relevant Customer Due Diligence data upon request by the firm. It should be noted, that business is not permitted to engage in payable through accounts. Any waiver can only be granted by Compliance and the CEO, jointly.
• Specifying clearly the Bank's own responsibilities and those of the correspondent institution under the banking correspondence agreement.
➢ ATTICA bank shall not establish or continue correspondent banking relationships with shell banks or continue correspondent banking relationships with banks that are known to allow their accounts to be used by shell banks. A shell bank is an entity incorporated in a jurisdiction where it has no physical presence involving meaningful decision-making and management, and which is not part of a financial conglomerate. Business shall request all banks abroad with which they are going to establish correspondent banking relationships to complete and sign a questionnaire stating their AML/CFT policies and procedures (e.g., the Wolfsburg Group questionnaire).

5.1 Customer and non-customer screening

Compliance must ensure that names of the customer, connected parties and suppliers are screened prior to account opening, and especially the customers daily, (automatically against international sanctions lists such as the OFAC/SDN Lists), in response to changes in the customer
profile, KYC review or post updated to AML & CFT lists. At a minimum, names of the following must be screened against applicable screening lists:

- All new customers
- All existing customers
- The customer's legal representatives/physical persons, in the case the customer is a legal entity
- The customer's beneficial owner
- Connected parties of PEPs
- Transaction counterparties who are not the Bank's customer.

For further guidance on customer and non-customer screening, please refer to the Customer Acceptance Policy.

5.2 Transaction Monitoring

ATTICA shall established systems and procedures to monitor ongoing customer activity to identify unusual/ suspicious activities. The Bank monitors transactions undertaken during its customer relationship to ensure that the transactions are consistent with its knowledge of the customer, their business and risk profile.

Alerts generated from name screening and transaction monitoring rules and scenarios defined by the MLRO and the Head of Compliance are investigated on a timely manner, according to the procedures of the Bank.

Units should provide appropriate information to the MLRO such as: name of the person(s) involved (customer, beneficiaries, counterparties, etc.), nature of transaction and any supporting documents as requested to assist the review of generated alerts.

For further guidance on transaction monitoring, please refer to the Customer Acceptance Policy.

5.3 Other Sources of Monitoring Referrals

The AMLO also performs reviews and investigations on the basis of Authorities requests outside the automated monitoring tools the Bank has in place.

Sources of such investigations could be :

- Bank of Greece
- Ministry of Finance
- The Hellenic FIU
- Law enforcement authorities requests
- Independent Authority for Public Revenue (ΑΑΔΕ)

5.4 Account Use Monitoring

Personal Account Used for Business Purposes

ATTICA prohibits personal account usage for any business related activity. Any such violation shall be investigated by the AMLO and may result in the termination of the relevant Customer's relationship.

Third Party Account Usage

If it appears that the account is being used by any person other than the actual account holder or mandate holder and transaction is carried out on behalf of another person, vigilance is required, i.e. it becomes necessary to identify that person. The matter should be escalated immediately to the respective Branch / Business Manager and MLRO after obtaining the required information for taking final decision regarding the fate of the relationship.

Staff Account Monitoring

Monitoring of staff accounts for any unusual activities is managed by Internal Audit.

Source of funds for Cash Deposits
Following a risk-based approach in respect of cash deposits:
• Source of funds in excess of EUR 15,000 should always be inquired & recorded on the deposit slip. Branches should also monitor accounts for multiple over the counter cash deposits in a day cumulatively breaching the threshold and obtain source of funds accordingly.
• Cash withdraws over € 50.000 should be monitored
• Persons active in the commerce of goods conducting cash transactions >= € 10.000 in one or in several acts
• Legal entities whose total cash deposits or cash withdrawals exceed €300,000 during the previous calendar year.
• Name, contact number & a copy of the Identification Document of the depositor is to be captured for all Teller Cash Deposits that are performed by an individual(s) whose name does not appear on the account and is not an authorised person of the company's bank account.

6. Unusual and Suspicious Activity Reporting

Suspicious activity/transactions – Suspicious transactions are understood as transactions or activities giving rise to sufficient indications or suspicions of actual or attempted commission of the offences referred to in or of involvement of the customer or beneficial owner in criminal activities, on the basis of the assessment of data of the transaction (nature of transaction, financial instrument, frequency, complexity and value of the transaction, use or non-use of cash) and the person n (occupation, financial condition, transactional or business behavior, reputation, past record, level of transparency of customers who are legal persons, and other important characteristics)
• Involves funds derived from potentially illegal activities (i.e. the sale of drugs, a fraud or tax evasion)
• Is potentially intended to be used for illegal activities (i.e. funding acts of terrorism)
• Is intended to or is conducted in order to hide or disguise funds or assets derived from illegal activities (including, without limitation, the ownership, nature, source, location, or control of such funds or assets) as part of a plan to violate or evade any law or regulation or to avoid any AML & CFT regulation (i.e. purchase of real estate in a foreign country using illegal money with the intention to sell shortly after and repatriate funds)
• Is designed to evade AML & CFT regulations, for example, a cash reporting or other record keeping regulation (i.e. exporting funds through family members accounts)
It is important to note that in the context of the definition above, suspicion does not mean proof, rather where there is doubt beyond a reasonable, rational level.

Unusual transactions are understood as transactions or activities incompatible with the customer's or beneficial owner's profile (transactional, professional or business behaviour, financial condition) or have no apparent purpose or motive of a financial, professional or personal nature.
Failure by a member of staff to report a suspicious activity to AMLO is a criminal offence subject to applicable fines/penalties imposed by competent authorities and law enforcement in accordance with the prevailing laws and regulations.

Internal reporting process
Further to the alerts generated by the AML & CFT system used by the Bank, any staff that is suspicious of a certain transaction or series of transactions is obligated to report the suspicious transaction(s) to the AMLO through e-mail to the following mail address:
aml-co@atticabank.gr.
The staff should complete the AML & CFT Suspicious Transaction Report (STR) and include as much detail as possible on the nature of the transaction, the individual(s) and/or corporate clients concerned and the nature of the suspicion. The completed form should report sufficient information to facilitate the investigation. Suspicious transaction reports submitted to the AMLO or must include at least the following data:

Date
•Full particulars of the reporting branch or service
•All the available information on the customer and the transaction
•The date of conduct of the transaction and establishment of the business relationship and a full record of transactions

•Justification of suspicion of the transaction on the basis of indicative typology issued by BoG and any other scenarios included in the system for AML or CFT transaction monitoring purposes and
• In international transactions, the origin and course of the incoming or outgoing remittance.
On completion, the form should be signed and dated by the reporting employee.
The MLRO will review the report and advise (if deemed necessary) if any action is required by the reporting unit or proceed with the action.
NOTE: Where a staff is suspicious and makes an AML & CFT Suspicious Transaction Report, the staff must ensure that the customer is not to be informed nor be made aware of this.

Reporting to Authorities process

The MLRO is required to monitor transactions, identify unusual activity and report suspicious transactions to competent authorities. S/he must retain a record of all Suspicious Activity Reports/Suspicious Transaction Reports filed.
Suspicious report to the FIU is submitted electronically through a secure communication between the Commission and the bank. There are two types of reporting forms provided by the FIU:
• The AML Standard Suspicious Transaction Report
• The AML Consolidated Suspicious Transaction Report for Tax Evasion category only
This form allows for numerous clients to be reported with one, consolidated submission. This report should contain:
(i) any clients identified as having significant deviations between their annual declared income and their actual annual transactions and
(ii) any clients who have been requested to provide their tax clearance certificate and either they have refused to provide it or avoid providing it – despite the bank's requests.
All Units must also comply with the relevant processes and controls to report their knowledge or suspicion internally to the MLRO and keep evidence of such reporting.
If upon investigation, a Suspicious Activity Report/Suspicious Transaction Report is filed, or frequent alerts are generated for a customer, then the Bank shall evaluate the fate of its relationship with the customer.

6.1 De-risking – Relationship Exits

The Compliance Function, as per MLRO advice, may at any time instruct the termination of an existing relationship due to an observed Un-Acceptable risk criterion met as per existing policy and/or as part of the risk mitigation measures.
The decision to exit the relationship due to AML & CFT risks will be taken by a Client Acceptance Committee consisted of the Chief Compliance Officer, the Head of the Business Unit, the CEO and, if necessary, the Chief Legal Counsel.
For exceptional cases, escalation may be made to the AC and/ or BoD.
Exit Instructions to respective Business units will contain explicit steps on how to proceed. The respective business line is responsible for ensuring all appropriate steps are taken, including liaising with appropriate departments, such as Legal, Credit to ensure accounts are closed in a commercially reasonable timeframe and in accordance to local laws. Such communications are for Bank's internal use and should not be provided (voluntarily or otherwise) to customers.

6.2 Tipping Off

It is prohibited by law to inform the customer either directly or indirectly that the Bank has filed a Suspicious Activity Report/Suspicious Transaction Report against them. Units must ensure that all staff are aware of their obligations not to 'tip-off' the customer.
According the AML Law and Regulation: the Bank's personnel is prohibited to communicate that information was forwarded or asked or that a research is carried out for Money Laundering, to everyone who is involved or a third person.
Employees may be directly held accountable by competent authorities and law enforcement if found guilty of tipping off, which can be punishable by financial penalties and/or imprisonment

7. Resourcing

ATTICA is committed to ensure sufficiently skilled resources are in place within each Unit to execute the requirements defined within this Policy. Applying the Three Lines of Defense model requires resources with adequate knowledge of AML & CFT compliance across the Bank.

8. Reliance

Under Law 4557/2018, article 19, persons/entities obliged to exercise due diligence may rely on third parties to fulfill part of their obligations. Ultimate responsibility for the fulfillment of these obligations remains with the obliged persons/entities.
Third parties are the following:
(a) credit institutions,
(b) leasing companies,
(c) the factoring companies,
(d) portfolio investment companies,

e) fund management companies,

(f) investment firms,
(g) investment intermediation companies,
h) insurance companies,
(i) e-money institutions that have their headquarters in a Member State of the European Union or in a third country that is a member of the FATF.
Obligated persons/entities relying on a third-party part:
(a) Receive by the third party any information it has acquired, by implementing the appropriate due diligence to the customer and the beneficial owner as specified in the said Law
(b) Ensure that at their request, without delay, copies are transmitted to them, in printed or electronic form, of the documents the third party has acquired during in the implementation of the due diligence measures.

9. Regulatory and Management Reporting

➢ The MLRO shall prepare an annual report, which should be an important input for the assessment of the bank's compliance with AML/ CFT provisions. The annual report shall be communicated to the CEO, assessed by the Board of Directors, through the Audit Committee, and shall be approved and submitted during March each year to the Bank of Greece in electronic form or in a hard copy, accompanied by the results of the annual assessment of the adequacy and efficiency of the AML/ CFT policy carried out by audit

➢ On a six months basis the MLRO should prepare the AML reports included in BoG Act 2651/2012

➢ An annual reporting obligation to the Ministry of Finance exists for those clients identified as high risk for tax evasion by the end of April each year (POL 1192/2013).

10. Records Management

All records relating to compliance with this Policy must be retained in accordance with the Bank Record Retention Policy. For all significant decisions relating to the application of this Policy should be supported by reasonable logs to demonstrate the rationale on which they are based. Such documentation should be retained as deemed appropriate and for a minimum of 5 years from the date of the decision.
The Bank should be able to provide the basic information on the customer and relevant transactions upon request by the relevant Competent Authority(ies). The Bank maintains database that stores customer information and their respective transactions.
The Bank should set up a record management system. Customer files should be organized on a systematic manner to enable the Bank to respond to Competent Authority's requests in a timely manner.

11. Monitoring and Review

ATTICA shall ensure that appropriate processes, systems and controls are in place to monitor the adequacy and effectiveness of this policy and respective procedures. Adherence to this Policy is assessed by assurance activities undertaken by Business Units, Compliance and Internal Audit applying the 3 Lines of Defense model.

12. Training and Communication

Relevant employees and Staff implementing this policy and respective procedures must complete training prior to commencement of their responsibilities. Training should include the key requirements of this Policy, applicable laws and regulations, relevant enforcement themes

and particular AML & CFT risks faced by ATTICA by virtue of its geographic footprint, product mix and client type.
Training to all staff shall be provided by receiving the on-boarding package upon recruitment and at least on an annual basis. Non-completion of prescribed mandatory training may impact employee performance ratings. Training can be web-based learning, by physical presence, internal or external.
Specific training shall take place for the staff of the Compliance/AML function as required by Law.

Related Regulations

• Government Gazette of The Hellenic Republic Law 4557/2018,as applicable, implementing Directive (EU) 2015/849 of the European Parliament And Of The Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing
• BoG Act 2652/29.2.2012
• BoG Act 2577/09.03.06 (and additional Annex 4 Decision 231/4/13.10.06 of the Committee of Banking and Credit Issues)
• Banking and Credit Committee Decision 281/17.3.2009
• Banking and Credit Committee Decision 285/9.7.2009
• Banking and Credit Committee Decision 290/17.3.2009
• Banking and Credit Committee Decision 300/28.7.2010
• Credit and Insurance Committee Decision 94/15.11.2013
• Regulation (EC) No 2015/847 of the European Parliament and of the Council of 15 November 2006 on information on the payer accompanying transfers of funds
• EBA Guidelines under Articles 17 and 18(4) of Directive (EU) 2015/849
• FATF Guidance on Risk-Based Approach to Combating Money Laundering and Terrorist Financing
• FATF Guidance on Transparency and Beneficial Ownership
• The 40 revised constitutions (02/2012) of the unit of financier interference - FATF (Financial Action Task Force)
• The 8 special constitutions (2001) for the financing of terrorism from the Unit of Financier Interference FATF (Financial Action Task Force)

Sound Management of Risks Related to Money Laundering and Financing of Terrorism according to :
• Hellenic Republic AML, CFT and Sanctions Laws and Regulations
• United Nations Security Council (“UN”) Sanctions Regulations
• European Union (“EU") Sanctions Laws and Regulations
• U.S. Department of Treasury’s Office of Foreign Assets Control (“OFAC”) Sanctions Laws and Regulations

APPENDIX I

A. Risk Factors/Variabilities

A.1 The following is a non-exhaustive list of risk variables that obliged entities shall consider when determining to what extent to apply customer due diligence measures:

(i) the purpose of an account or relationship;
(ii) the level of assets to be deposited by a customer or the size of transactions undertaken;
(iii) the regularity or duration of the business relationship.

A.2 The following is a non-exhaustive list of factors and types of evidence of potentially lower risk:

(1) Customer risk factors:
(a) public companies listed on a stock exchange and subject to disclosure requirements (either by stock exchange rules or through law or enforceable means), which impose requirements to ensure adequate transparency of beneficial ownership;
(b) public administrations or enterprises;
(c) customers that are resident in geographical areas of lower risk as set out in point (3);

(2) Product, service, transaction or delivery channel risk factors:
(a) life insurance policies for which the premium is low;
(b) insurance policies for pension schemes if there is no early surrender option and the policy cannot be used as collateral;
(c) a pension, superannuation or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages, and the scheme rules do not permit the assignment of a member's interest under the scheme;
(d) financial products or services that provide appropriately defined and limited services to certain types of customers, so as to increase access for financial inclusion purposes;
(e) products where the risks of money laundering and terrorist financing are managed by other factors such as purse limits or transparency of ownership (e.g. certain types of electronic money);

(3) Geographical risk factors:

(a) Member States;
(b) third countries having effective AML/CFT systems;
(c) third countries identified by credible sources as having a low level of corruption or other criminal activity;
(d) third countries which, on the basis of credible sources such as mutual evaluations, detailed assessment reports or published follow-up reports, have requirements to combat money laundering and terrorist financing consistent with the revised FATF Recommendations and effectively implement those requirements.

A.3. The following is a non-exhaustive list of factors and types of evidence of potentially higher risk:

(1) Customer risk factors:
(a) the business relationship is conducted in unusual circumstances;
(b) customers that are resident in geographical areas of higher risk as set out in point (3);
(c) legal persons or arrangements that are personal asset-holding vehicles;
(d) companies that have nominee shareholders or shares in bearer form;
(e) businesses that are cash-intensive;
(f) the ownership structure of the company appears unusual or excessively complex given the nature of the company's business;

(2) Product, service, transaction or delivery channel risk factors:
(a) private banking;
(b) products or transactions that might favour anonymity;
(c) non-face-to-face business relationships or transactions, without certain safeguards, such as electronic signatures;
(d) payment received from unknown or un associated third parties;
(e) new products and new business practices, including new delivery mechanism, and the use of new or developing technologies for both new and pre-existing products;

(3) Geographical risk factors:
(a) without prejudice to Article 9, countries identified by credible sources, such as mutual evaluations, detailed assessment reports or published follow-up reports, as not having effective AML/CFT systems;
(b) countries identified by credible sources as having significant levels of corruption or other criminal activity;
(c) countries subject to sanctions, embargos or similar measures issued by, for example, the Union or the United Nations;
(d) countries providing funding or support for terrorist activities, or that have designated terrorist organizations operating within their country.

B. Assessment of country risk for AML/CTF purposes, may be based on the following criteria:
I. Announcements by FATF concerning countries or territories that do not comply or comply inadequately with its recommendations;
II. Country assessment reports issued by FATF, regional bodies that have been established and operate according to its standards (e.g., Council of Europe Moneyval Committee), the

International Monetary Fund and the World Bank;
III. List of countries or jurisdictions which, according to the Common Understanding of the Committee for the Prevention of Money Laundering and Terrorist Financing, which assists the European Commission, have equivalent AML/CTF systems to the EU (see paragraph 97 for the 'equivalence' lists Greece lines of business follow);
IV. Countries characterized by FATF as non-cooperative or tax havens;
V. Inclusion in the EU, UN and OFAC lists;
VI. FATF membership;
VII. Implementation of EU directives;
VIII. Implementation of the Wolfsburg Principles;

Useful links to decisions issued by the Independent Authority for Public Revenue (ΑΑΔΕ) related to country risk:

- "Determination of the states having a preferential tax regime" based on the provisions of paragraphs 6 and 7 of article 65 of Law 4172/2013 for tax year 2022 https://www.aade.gr/egkyklioi-kai-apofaseis/1205-19-12-2023
- "Determination of non-cooperative states" on the basis of the provisions of paragraph 3 of Article 65 of Law 4172/2013 for the year 2021. https://www.aade.gr/egkyklioi-kai-apofaseis/1028-07-03-2023

APPENDIX II

Criminal Activity: Crimes according Article 4 - – Law 4557/2018 - Basic offenses (Article 3 (4) of Directive 2015/849)

According Article 4 - – Law 4557/2018, "basic offenses" means the following:
(a) The criminal organization, as defined in Article 187 CC,
(b) Terrorist acts and terrorist financing as defined in Article 187a of the FR,
(c) Bribe and bribery of an official as defined in Articles 235 and 236 of the CC,
(d) Inter-influence trading and bribery and bribery in the private sector, as defined in Articles 237a and 237b of the CC,
(e) Bribery and bribery of political and judicial officers as defined in Articles 159, 159a and 237 of the CC,
(f) Trafficking in human beings, as defined in Article 323a,
(g) Computer fraud, as defined in Article 386a of the CC,
(h) Trafficking in human beings, as defined in Article 351 CC,
(i) The offenses provided for in Articles 20 to 23 of Law 4139/2013 (A 74);
(j) The offenses provided for in Articles 15 and 17 of Law 2168/1993 (A 147),
(k) The offenses referred to in Articles 53, 54, 55, 61 and 63 of Law 3028/2002 (A 153);

(l) The offenses provided for in Article 8 (1) and (3) of Dec. 181/1974 (A 347),
(m) The offenses provided for in Article 29 (5) and (8) and Article 30 of Law 4251/2014 (A 80);
(n) The offenses referred to in fourth and sixth articles of Law 2803/2000 (A 48);
(o) The stock exchange offenses provided for in Articles 28 to 31 of Law 4443/2016 (A 232);
(p) Offenses: (aa) tax evasion provided for in Article 66 of Law 4174/2013 (A 170) with the exception of the first subparagraph of paragraph 5, (bb) smuggling provided for in Articles 155 to 157 of Law No. (C) the non-payment of debts to the State provided for in Article 25 of Law 1882/1990 (A 43), with the exception of paragraph 1 (a), and the non- payment of debts resulting from pecuniary sanctions or fines imposed by the courts or by administrative and other authorities,
(q) The offenses provided for in Article 28 (3) of Law No 1650/1986 (A 160); (r) any other offense punishable by a custodial sentence of a minimum of six (6) months and from which an asset benefit arises.

APPENDIX III
FATF Latest Announcements and Jurisdictions

FATF MEMBERS:

- Argentina
- Australia
- Austria
- Belgium
- Brazil
- Canada
- China
- Denmark
- European Commission
- Finland
- France
- Germany
- Greece
- Gulf Co-operation Council
- Hong Kong, China
- Iceland
- India
- Indonesia
- Ireland
- Israel
- Italy
- Japan
- Korea
- Luxembourg
- Malaysia
- Mexico
- Netherlands
- New Zealand
- Norway
- Portugal
- Russian Federation *
- Saudi Arabia
- Singapore
- South Africa
- Spain
- Sweden
- Switzerland
- Türkiye
- United Kingdom
- United States

* FATF suspended membership of the Russian Federation on **24 February 2023**

In order to protect the international financial system from ML/FT risks and to encourage greater Compliance with the AML/CFT standards, the FATF identified jurisdictions that have strategic Deficiencies.
According to BoG's Decision 281/5/17.03.2008 – Chapter 5.15.9 and 5.15.10 the Bank should take all necessary measures during the collaboration with Individuals and Legal Entities which are based in the following countries.
Especially while creating collaboration with a Bank as a Correspondent it is obligated to fulfill the Wolfsberg's Group Questionnaire and to identify all the real holders of those institutions.

Jurisdictions subject to a FATF call on its members and other jurisdictions to apply countermeasures to protect the international financial system from the on-going and substantial money laundering and terrorist financing (ML/FT) risks emanating from the jurisdictions*:

- ***Iran***
- ***Democratic People's Republic of Korea (DPRK)***
- ***Myanmar***

Transactions from/to Iran and Korea are not accepted

Jurisdictions with strategic AML/CFT deficiencies.

The FATF calls on its members to consider the risks arising from the deficiencies associated with each jurisdiction, as described below:

- **Haiti**
- **Albania**
- **Barbados**
- **Burkina Faso**
- **Cayman islands**
- **Cameroon**
- **Croatia**
- **Democratic Republic of the Congo**
- **Gibraltar**
- **Jamaica**
- **Jordan**
- **Mali**
- **Mozambique**
- **Nigeria**
- **Panama**
- **Philipines**
- **South Africa**
- **Senegal**
- **Syria**
- **South Sudan**
- **Tanzania**
- **Turkey**
- **Uganda**
- **Yemen**
- **United Arabic Emirates**