BANK OF AFRICA EUROPE

# SUMMARY OF POLICIES WITH REGARD TO THE PREVENTION OF MONEY LAUNDERING AND THE FINANCING OF TERRORISM

## BANK OF AFRICA EUROPE

*April 2025*

BANK OF AFRICA EUROPE

TABLE OF CONTENTS

## INTRODUCTION

BANK OF AFRICA EUROPE, incorporated in 1994 as a Spanish bank and registered with the Bank of Spain under number 0219, is supervised with regard to the prevention of money laundering by the Executive Service of the Commission for the Prevention of Money Laundering and Monetary Offences (SEPBLAC).

Spain is a member state of the European Union and as such has transposed to its legislation the EC Directives relative to the prevention of money laundering and the financing of terrorism. Spain is also a member of the Financial Action Task Force (FATF).

As European bank, BANK OF AFRICA EUROPE is submitted to all European laws concerning the prevention of money laundering and financing of terrorism. Local regulation is also respected, mainly:

- Spanish Law 10/2010, of 28 April 2010, on the Prevention of Money Laundering and Terrorist Financing.

- Royal Decree 304/2014 of 5 May.

BANK OF AFRICA EUROPE has designed and implemented a program for the prevention of money laundering and the financing of terrorism based on policies and procedures which are mandatory for all the areas of our bank.

In this sense all guidelines and recommendations from FATF- GAFI, Egmon Group, SEPBLAC and Bank of Spain have been included.

## 1. GENERAL PRINCIPLES OF THE AML / TF POLICIES

As stated in our Manual for the Prevention of Money Laundering and Terrorism Financing and the Technical Procedures for development and implementation, the principles that govern our activity in the field:

a. **Risk approach**, through the preparation of reports that describe and evaluate the risk exposure of AML / TF in relation to our activity.

b. **Sensitization of senior management and the management body**, which knows the risks in the matter and ensures that appropriate measures are taken to mitigate those risks.

c. **Focus on generalized prevention**, including not only the technical unit of prevention and control units, but also the own business network as the first line of defense.

d. **Feedback derived from the steady communication between the technical units and the**

**business units**, related to the risks in which they may be involved and the measures necessary to mitigate them.

e. **Universality** that guarantees that the protocols are applied to all clients, operations and business scope without exception.

f. **Adaptation to the specific business** of our entity.

g. **Pillars of prevention**: determination of real ownership, knowledge of the origin of the funds and the consistency of the operation.

h. **Reinforced monitoring** of new customers, products or services.

i. **Practical document and quick method of implementation** of the current standards.

j. **External reviewers of the AML/TF** system effectiveness.

k. **Updates and review of registered procedures**.

## 2. POLICY FOR THE ACCEPTANCE OF CUSTOMERS.

In compliance with the due diligence regulations regarding customers, specific rules and procedures are in place to regulate the policy for the acceptance of commercial relationships. The policy for acceptance of customers is adapted to each type of customer according to the risk assignation.

For the purpose of controlling the risk of ML/TF, the Bank will not accept the following categories of customers:

- ✓ Persons or entities known to be linked to terrorist or criminal activities or money laundering operations.
- ✓ Persons or entities included in the Council Regulation EC 881/2002 of 27 May 2002.
- ✓ Persons or entities in respect of which it has not been possible to comply with the measures for the formal identification and identification of the beneficial owner as provided for in the regulations have not been complied with.
- ✓ Persons or entities are subject to forbidden operating, as per their inclusion on the relevant lists for links to terrorism or other reasons.
- ✓ Persons or entities of which there is insufficient knowledge (which must include, in any case, knowledge of the origin of the funds) to guarantee the legality of transactions, as provided for in the regulations.
- ✓ Casinos, gaming companies, companies related to gambling or officially licensed betting establishments
- ✓ Customers related to the production or distribution of arms and other items of a military nature.

- ✓ Nuclear-related customers.
- ✓ Natural or legal persons whose object or activity is real estate development, agency, commission or intermediation in the purchase and sale of real estate.
- ✓ Persons or entities that intend to carry out operations derived from activities related to games of chance, betting or similar activities without having the necessary requirements, in particular the corresponding official authorization.
- ✓ Philatelic and numismatic investment.
- ✓ The marketing of lotteries or other games of chance in respect of prize-paying transactions
- ✓ Customer transactions involving virtual currencies, bearer cheques or involving a cash movement of more than 3.000 Euros.
- ✓ Cash transactions supported by banknotes of 200 and/or 500 Euros face value.
- ✓ Transactions involving 'NESTING' or mail clearing, which means that the correspondent bank is indirectly providing services to credit institutions other than the client institution.
- ✓ Shell banks or insufficiently justified regulatory jurisdiction.
- ✓ Clients related to the adult entertainment industry.
- ✓ Person under 18 years of age.
- ✓ Legal persons and other instruments of risk jurisdictions.
- ✓ Insufficient information or documentation.

In their admission, clients will be classified by the level of risk in 3 levels (high / medium / low), depending on the risk of AML / TF inherent in their legal form and activity. Thus, depending on the risk and in compliance with the due diligence rules, the necessary measures are established to monitor their activity and update their file and the commercial relationship. The measures of diligence will be adapted to every type of client based on the assignment of risk (simplified, normal or reinforced diligence). The documentation required for the account opening for natural and legal persons requires first, the understanding of their activity and the source of funds with the requirement to support all of it with the relevant documentation for each type of person. Secondly, the tax residence must be disclosed and in the case of legal entities, the ultimate beneficiary owner too.

## 3. POLICY FOR THE IDENTIFICATION OF THE CUSTOMER.

Specific rules and procedures are in place to ensure the identification and knowledge of the customer.

It should be mentioned that the bank has specific procedures to identify politically exposed persons (PEPs) or their direct family members or close collaborators.

When there is a relationship with a PEP the following Enhanced Due Diligence is undertaken: Update of the data obtained during the customer acceptance process, increase of the periodicity of the document review

process, obtaining of additional information about the client (real owner, purpose and nature of the business relationship, origin of the funds, patrimony of customer, purpose of the transaction), obtaining executive authorization to establish or maintain the business relationship or execute the operation, within others measures.

## 4. POLICY FOR IDENTIFICATION OF THE BENEFICIAL OWNER.

Pursuant to the Law 10/2010 of 28 April on the Prevention of Money Laundering and the Financing of Terrorism, BANK OF AFRICA EUROPE has implemented a procedure for identification of the beneficial owner

The bank adopts the appropriate measures in order to verify their identity prior to the establishment of business relations or the execution of whatsoever transactions.

## 5. POLICY REGARDING KNOWLEDGE OF THE CUSTOMER.

Our bank has established rules, procedures and internal controls in order to obtain full knowledge of its customers, their activities and the purpose of their business relationship.

For business reasons and to prevent certain suspicious activity, the offices and commercial collaborators must have enough knowledge of the activity carried out by the customer and whether this justifies the operations and financial flows that pass-through BANK OF AFRICA EUROPE.

This knowledge should be considered one of the necessary conditions for the commencement of commercial relationships with new customers, thus eliminating the possibility for the opening of spontaneous accounts in the bank, without previous information being provided to the senior management of our bank.

Our policy for knowledge of the customers is a basic element of the risk management and control procedures of the bank. This is based on a focus on a risk and continuous monitoring, assisting us to manage more prudently. It is to be emphasized that automatic mechanisms are in place to detect the inclusion of persons blacklisted of the United Nations, the European Union[1] or the OFAC[2], both in the customer acceptance process and in daily operations.

As mentioned before, our AML Policy establishes several types of customers, which by their characteristics are not admissible. Once the client is admitted, the internal procedure includes the identification of risk factors and the methodology to categorize clients. According to the Bank risk-based approach, clients are classified as per the following risk levels and updating process frequency: High Risk (every 12 months); Medium Risk

[1] Source: http://eeas.europa.eu/cfsp/sanctions/consol-list/index_en.htm
[2] Source: http://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/fse_list.aspx

(every 18 months); Low Risk (every 24 months); New Clients (activity is reviewed in 6 months since the beginning of the relationship)

The factors considered when undertaking the assessment of risk are the profile of the customers and their activities, jurisdiction, countries or geographic areas in which it undertakes business, products, services and activity profiles, distribution channels and business partners, complexity and volume of transactions, development of new products and new business practices, source of funds, shareholders, annual accounts, and share capital.

## 6. POLICY FOR ACCEPTANCE OF CORRESPONDENT BANKS.

Policies are in place for the acceptance of banks with which correspondence is established. These policies and processes cover from the compilation of information regarding the correspondent banks to the analysis based on the risk focus.

To carry out the study of the banks, the following documentation is established:

- Copy of last annual report;
- Copy of last audited accounts;
- Copy of activity license issued by the Central Bank of the country of registration;
- Copy of commercial registration form;
- Copy of its bylaws;
- List of its shareholders and real owners;
- List of the members of its Board of Directors and its Executive Committee, in addition to their CVs and Passports;
- Copy of their AML policy;
- BANK OF AFRICA EUROPE ´s AML Questionnaire and the latest version of the Wolfsberg questionnaire filled and signed;
- Certification of the US Patriot Act and W8-BEN-E form; and,
- FATCA number (W-8BEN).
- AML Audit
- Last signature book

The bank cannot establish or maintain correspondence relationships with shell banks or with banks that are known to allow the use of their accounts by shell banks (article 13 Law 10/2010).

Neither correspondence relationships may be established or maintained that, directly or via a sub- account, allow the execution of transactions by the customers of a represented bank (article 13 Ley 10/2010).

## 7. INTERNAL ORGANIZATION.

BANK OF AFRICA EUROPE has an internal organization that allows to guarantee the homogeneous fulfillment of the normative policies regarding PBC / FT:

- **The Technical Unit of AML / TF (UTPBC)** is the specialized body in the matter and is dedicated to the analysis of information related to policies, procedures, clients, operations and relevant products and services for the prevention and mitigation of AML/ TF risk.

- **The Internal Control Body (OCI),** as the representative body of the different business areas affected by the AML / TF regulations together with the Management of the Entity. It is responsible for making decisions regarding the directives in the matter, admission of clients, analysis of suspicious transactions, decision of communications to the SEPBLAC, collaboration with the SEPBLAC Commission, etc. In addition, is in charge of verifying the proper functioning and effectiveness of the measures and procedures.

- **The representative towards the SEPBLAC** is the person in charge of communication and direct contact at technical level with the OCI and at institutional level with the SEPBLAC. It possesses global access to all the information and files which is necessary for monitoring and controlling the issue.

- **Senior Manager Responsible for AML/TF:** is aware of the impact of ML/TF risks on their business-wide risk profile, and ensure in particular in relation to the implementation of policies, controls and procedures to mitigate and manage effectively the risks of ML/TF are adequate and proportionate.

- **The Senior Management of the Entity**, responsible for the policies and measures implemented in the matter, which implies having full knowledge of the specific risks of the Entity, as well as training in the subject. In addition, the Board of Directors is the ultimate responsible for ensuring AML scheme and approving Policies in of AML / TF, the Risk Self- Assessment Report in what regards the ML / FT, the Annual Report, the Internal Verification Report or any other document or report that is thus determined.

## 8. TRAINING PLAN.

As established by current regulations on the prevention of money laundering, the continuous and permanent training of the personnel in this matter constitutes one of the fundamental objectives of the Bank in order to apply adequate policies for the prevention of money laundering.

Therefore, Management, with the collaboration of the Internal Control Body (OCI), prepares and promotes annual training plans for its employees in order to communicate the new legal requirements that arise, to explain the internal procedures on this matter and to achieve adequate competence in order to detect transactions related with money laundering.

The training programs will consider international rules and local legislation against money laundering and the financing of terrorism, as well as the internal rules and procedures intended to fight money laundering and the financing of terrorism, including the ways for recognizing and reporting suspicious activities.

The OCI must approve the training plan and may inform the employees of the regulatory modifications in this matter as well as all the new modalities, techniques or procedures detected that are susceptible of being used in the fight against money laundering.

## 9. INTERNAL AND EXTERNAL CONTROLS

AML control unit is under Compliance Department organization, unit which is submitted to the supervision of the **Joint Risk and Audit Committee (CMAR)**, delegated committee of the Board of Directors, ultimately responsible for the AML/FT scheme.

Additionally, the Entity has entrusted to **the Permanent Control Unit**, monitoring the most immediate processes and risks in the matter, this task is included in its planning and the recommendations, corrections or improvements that must be made are reported to the departments affected, the senior management and the OCI. Every six months, it presents a report to the CMAR where these elements are included.

On the other hand, **the Internal Audit deparmente** of the bank in its Audit Plan supervises and verifies the application of the guidelines on the established procedures, the operations and the procedures, concluding and issuing an opinion on its effectiveness and adjustment.

Every year, an **independent external expert in AML/FT** conducts an examination that assesses the adequacy of the policies, procedures and manuals regarding AML / TF, in accordance with the regulatory requirements established.

## 10. INTERNAL REPORTING OF SUSPICIOUS TRANSACTIONS

Following European regulation and internal rules and procedures for reporting, any employee who detects a transaction suspicious of money laundering must communicate it to the UTPBC in which will be evaluated if is necessary to carry on to OCI, with previous urgent analysis by UTPBC, which will analyze the transaction urgently and determine its reporting to the SEPBLAC when it presents signs of suspicion.

Any employee or stakeholders can make use of the Denunciation Channel, in application of the Spanish regulation related to whistleblowing protection.

## 11. REPORTING OF TRANSACTIONS TO THE AUTHORITIES

Pursuant to the reporting obligations of entities subject to anti-money laundering obligations vis-à- vis the SEPBLAC, the Money Laundering Prevention Unit will issue the communications to the SEPBLAC.

This obligatory and systematic reporting consists of sending to the Executive Service on a monthly basis the transactions that meet the criteria established in paragraphs a), b), c), d), e) and f) of article 27.1 of the Regulations of the Law 10/2010, approved by Royal Decree 304/2014.

Likewise, the Money Laundering Prevention Unit will develop and implement adequate controls in order to detect any transaction likely to be suspicious.

To generate such information, the Money Laundering Prevention Unit will use a system of defined alerts and filters, as well as a catalog or registry of types of transactions related with ML/TF, in order to detect any possible transaction with traces of or related to ML/TF.

BANK OF AFRICA EUROPE systems has parameterized a series of alerts on transaction/customers that have been defined internally by the Compliance team. If it detects an operation/customer that leaves the normal pattern expected, the system notifies the Compliance department to review the transaction. The Compliance department receives also, suspicious cases reported by internal departments. When the Compliance department receives suspicious cases (from the system or from other departments) his mission consists in investigating in more detail these suspected cases of money laundering. While undergoing investigation, the Compliance team might request additional information related to the transaction or case reported, to assist in the investigation. The case is then reported to the OCI for discussion with a report where the findings of the investigation are disclosed. The Head of Compliance presents the case to the OCI, which studies and discusses all the facts. If a serious doubt persists and the case investigated is a potential attempt to launder funds, the case is immediately reported to SEPBLAC (Spanish regulator).

## 12. CONSERVATION AND FILING OF DOCUMENTS.

The period established for the conservation of documentation is ten years, complying with the provisions of the Law 10/2010.

The said documentation or information will be adequately filed to facilitate its location and guarantee its confidentiality.

The Bank makes back-up copies on a monthly basis, storing said copies in a location other than the address of the Bank.

### 13. PATRIOT ACT.

Pursuant to the requirements established by the United States Law "USA PATRIOT ACT[3], all banks that are domiciled outside the United States and which wish to establish or maintain relationships of international correspondence with a US bank or broker/dealer or maintain a U.S. DOLAR account , are obliged to provide certain information regarding the nature of their business and the degree of supervision to which they are subject.

### 14. W-8BEN or W-8BEN-E (FATCA NUMBER - Foreign Account Tax Compliance Act)

Form W-8BEN must be completed by any person (individual W8BEN or legal entity W-8BEN-E) who is not a U.S. citizen and who receives income from a U.S. source. payer.

In this sense our Entity complies with American regulation, being registered in IRS as Reporting Financial Institution under a Model 1 IGA.

[3] Certificate corresponding to the USA Patriot Act, pursuant to sections 313 and 319 of the Patriot Act (Public Law 107- 56)