

Statement of AML policy

Optima bank SA ("Optima bank" or the "Bank"), headquartered in Athens, Greece (EU member), is regulated by the Bank of Greece (www.bankofgreece.gr) and operates in Greece, through its branch network.

Optima bank complies with all the provisions of national anti-money laundering legislation, as particularly outlined in Law 4557/30.07.2018 on the prevention and combating of money laundering and terrorist financing, as in force, incorporating in Greek law the provisions of relevant EU Directives (e.g. 2015/849, 2018/843 and 2018/1673) of the European Parliament and of the Council, as well as with international best practices.

Policies and procedures

The AML/CFT policies of Optima bank are reviewed on a regular basis and approved by the Board of Directors, being in line with the aforementioned framework, the respective sanctions regulations, supervisory authority decisions and guidelines, as well as the FATF recommendations.

AML/CFT risk management

Optima bank has established a comprehensive AML/CFT compliance program designed in accordance with applicable laws, regulations and international best practices, adopting a risk-based approach. This program is tailored and encompasses several key elements, including but not limited to the following:

- Risk-based customer due diligence applied to all clients in accordance with applicable laws and regulations, including the identification and verification of their identity, as well as the identity of beneficial owners and proxy holders. Enhanced due diligence is applied to clients categorized as "high-risk customers", pursuant to the Bank's policies and procedures. The keystone of the due diligence procedure consists of the Know Your Customer (KYC) principle and is applied to every client, without exceptions.
- AML/CFT Training Program, tailored according to each business unit's needs, in order to enhance staff awareness of AML/CFT related matters.
- Transaction Monitoring automated mechanism to track customer transactions and ensure timely reporting to competent regulatory authorities when required.
- Policies preventing transactions or activities involving individuals, entities or organizations, subject to comprehensive EU, UN, OFAC, UKHMT sanctions, with heightened surveillance on financial institutions or territories potentially linked to terrorist organizations.
- Ensuring customer and transaction records are maintained for a minimum of five (5) years post-business relationship termination or transaction execution.

Prohibited business relationships

In accordance with the Bank's applicable policies, certain transactions and types of customers are deemed prohibited and thus not accepted by the Bank. Namely:

Prohibitions related to transactions

Optima bank has strict policies regarding transactions in order to ensure compliance with national and international laws and regulations and prevent illegal activities. The following transactions are deemed prohibited:

- transactions related to money laundering, terrorism financing, human trafficking, political corruption and other fraudulent activities, as prescribed in applicable legal and regulatory framework
- transactions violating sanctions imposed by the EU, UN, OFAC, UKHMT, Greek authorities and other relevant bodies.
- transactions involving parties in high-risk geographic areas are also restricted based on assessments of AML/CFT, sanctions, tax, and corruption risks.

Prohibitions related to customers

Optima bank will not initiate or sustain a relationship with any of the following customer types, including but not limited to the following:

- Shell Banks or Financial Institutions that allow their accounts to be used by shell banks
- Shell companies / Companies having "Bearer Shares"
- Individuals or entities subject to restrictive measures based on EU, UN, OFAC, UKHMT or local authorities
- Individuals or entities involved in illegal activities, pyramids, pedophilia, pornography
- Customers involved in fraud against third parties

Customer identity verification policy

As part of Optima bank's commitment to compliance with the applicable legislative and regulatory framework, thorough verification procedures are implemented to confirm the identity of prospective customers, whether individuals or legal entities, prior to engaging in business relationships or transactions. This process includes ongoing updates to customer records and reasonable risk-based measures to understand ownership and control structures for legal entities.

Verification involves the collection of all relevant valid and up-to-date information to establish the customer's identity, financial and business profile and the intended nature of their relationship with Optima bank.

Additionally, screenings are conducted to determine whether a customer appears on lists of restricted entities or individuals subject to sanctions, and whether they are qualified as politically exposed persons (PEPs). Reputation assessments are also undertaken to gauge their standing within the market and community.

Customer profile

To ensure the creation of a robust KYC, essential data from trustworthy sources are gathered and compiled to establish a financial and business profile for each customer, including the origin of funds, the source of funds and the nature of their intended relationship with the Bank.

Risk-based customer classification

Each customer is assessed and classified according to a dynamic risk-rating process, which considers all available demographic, professional and business-related information, taking into account all applicable framework requirements while adhering to the established countries lists issued by international organizations (e.g., FATF).

Requests for Information

To uphold the applicable KYC obligations, our team periodically requests information from clients and third parties regarding their business activities. In addition, clients can be asked to provide:

- details and/or justification regarding specific account activity or transactions
- additional information regarding their business and financial profile

Upon detection of transactions that seem to be suspicious or unusual based on the existing information, further investigation is initiated. If the transaction still remains unjustifiable, it shall be reported to the competent FIU, according to the provisions of the applicable legislative and regulatory framework and the internal procedures of the Bank.

Restrictions can be imposed on the use of accounts in case of suspicious or unusual transactions and/or behaviors.

Any inquiries related to this policy should be addressed to the Relationship Manager. Clients and third parties are required to comply with the above-mentioned obligations, as non-compliance with our internal policies and risk appetite may result in payment rejection, account closure and/or termination of the business relationship.