

Knowing your Customer and AML /CFT Policy

The KYC & AML/CFT Policy of the Bank is issued with the aim to ensure the carrying out of banking activities in compliance with the national and international legal requirements and the legislation regarding Anti Money Laundering and Terrorism financing, to ensure the observance of the prudential, sound banking practices and in order to promote high ethical and professional standards and prevent the Bank from being used intentionally or unintentionally in illegal or criminal activities performed by its customers.

Description and process of Money Laundering

“**Money Laundering**” is a process to convert the unlawful proceeds of a criminal activity into funds with an apparently legal source, whereby the undiscovered launderers can subsequently enjoy the fruit of their crime.

In the process of money laundering, the laundered disguises the illegitimate nature of the sources of that income to make appear legitimate and banks are used as intermediaries for the deposit, transfer or investment of funds derived by criminal activity. Money laundering is a vital component of arms and drug trafficking and other illegal operations (i.e., terrorist activity, thefts and fraud, robbery, forgery and counterfeiting, illegal deposit taking, blackmail, bribe and tax evasion).

The money laundering activity may range from a simple funds transfer to diverse and complex process. The money laundering cycle starts with an illicit activity and goes on through three steps including placement, layering and integration as detailed below:

- Placement:** the physical disposal of the proceeds of illegal activity, depositing cash;
- Layering:** separating proceeds of the illegal activity from the source through complex financial transactions (converting cash to any sort of banking transaction, transferring funds into several accounts);
- Integration:** providing an apparent legitimate explanation for illicit Proceeds. Proceeds are placed into the system and legalized as normal business earnings, purchase of real estate, false trade invoices, collateral backed loan, L/C schemes, etc.

FIU – Anti-Money Laundering National Office (ONPCSB)

As per the provisions of the Anti-Money Laundering, the National Office for the Prevention and Combat of Money Laundering (ONPCSB), has been established is the Romanian FIU. The ONPCSB is subordinated directly to the Romanian Government.

The objective of the Anti-Money Laundering Office is to prevent and combat money laundry activities and terrorism financing. Therefore, it receives and analyzes information notifying the

Legal Authorities whenever necessary. The ONPCSB is entitled to request any kind of information from the Bank and the Bank is obliged to comply with the request of the ONPCSB, as per the provisions of the above Law.

There are mandatory reports, the Bank must send daily to FIU as Cash Transactions Report and External Transactions Report and the Suspicious Transaction Report to be sent to FIU each time a suspicious activity on customer accounts are identified.

The suspicious character of a banking transaction come from the unusual way it is performed in relation to the transactional profile and current activities of a customer. Suspicions arise from clues or suppositions about a transaction linked to money laundering. Suspicions may be on personal and subjective, and generates mistrust in the person or persons performing the transaction, and doubt regarding the correctness and lawfulness of facts or of the honest intentions of the person involved.

Anti-money laundry policy of the Bank

General Principle

Policy is defining the elements and measures to be taken into consideration by the employees involved in all Bank areas, in order to identify, measures and mitigate the ML/FT risks.

The Management body of the bank appoints Compliance Officer, who is authorized for overall responsibilities for AML/CFT function and has full authority for ongoing monitoring of the fulfillment of all AML/CFT duties by the bank and also is the contact point regarding all AML/CFT issues for internal and external authorities including supervisory authorities and FIU (ONPCSB).

Adequate transactions monitoring tools

The Bank has in place adequate monitoring tools and IT applications in order to ensure an effective AML/CFT activity and enable the bank to undertake trend analysis of transaction activity and to identify unusual business relationship and transaction in order to prevent ML or FT.

The existing IT monitoring system uses adequate parameters defined based on the national and international standards and following the guidelines issued by FIU. Also there are defined and implemented specific scenarios and alerts as additional monitoring tools in order to identify unusual transactions on customers' accounts.

Know your customer (KYC)

Know your customer process is the important part of the AML/CFT Process. The Bank shall open accounts for its customers in accordance with the Current Account Procedure.

The account opening file shall include all documentation as per the Current Account Procedure and any further documentation considered as necessary by the Bank Officers, the Legal Division or the Managers.

Customer Acceptance Policy (KYC standards)

Key elements of KYC standards

The Bank has issued adequate internal regulations and guidelines that promote high standards of knowing the customer and has defined **key elements** concerning:

- (1) Customer acceptance rules;
- (2) Customer due diligence;
- (3) Customer identification;
- (4) Customer risk assessment;
- (5) on-going monitoring of high risk accounts;
- (6) Monitoring accounts activity for AML/CFT perspective;
- (7) Termination of relationship;
- (8) Correspondent banking accounts;
- (9) Knowing your customer training programs.

The Bank shall only enter into **correspondent relationships**, or continue such relationships with banks that have implemented adequate know your customer and money laundering prevention policies and practices. The correspondent banking relationship will not be established with shell banks and financial institutions if there is any doubt about whether FI has a correspondent banking relationship with shell banks or not.

The Bank **does not open or operate anonymous or fictitious name accounts** for which the holder's identity is not known and stated accordingly.

The Bank's customer identification process is defined by Know your Customer internal procedure or guidelines and includes the following:

- **Identifying** of customer;
- **Verification** of customer identity;
- **Identifying the real beneficiary** of the funds;
- **Verification of real beneficiary** identity;
- **Establishing the transactional profile** of the customer;
- **Determining the source of funds** that the customer will deposit / trade by account/s opened;
- **Monitoring the transactional activity** of the customer - permanent activity.

Policy for identifying the Correspondent Financial Institutions

The bank while entering into any kind of correspondent banking arrangement shall gather sufficient information to understand fully the nature of the business of the correspondent / respondent bank. Information on the other bank's management, major business activities, level of AML/CFT is required.

The bank should only establish relationships with credit institutions abroad that are efficiently supervised by the competent authorities, and that have efficient know your customer programs.

The bank should decline entering correspondent relationships, or continuing such relationships with a credit institutions that is registered in a jurisdiction where the same does not have a physical presence, namely the management of the business and the official documents of the institution are not located in such jurisdiction, and to pay special attention when continuing correspondent relationships with a credit institution being located in a jurisdiction where there are not regulated

know your customer requirements, or that was identified as non-cooperating as regards money laundering fighting.

When establishing correspondent relationships, the bank should consider certain factors including without limitation the following:

- Information about the management if the correspondent credit institution, about their basic business, where it is located, and the efforts of the same to prevent and detect money laundering deeds;
- The purpose the correspondent account is opened for;
- The identity of any third party to use the correspondent banking services;
- The status of the regulations, and of the banking supervision system in the origin country of the correspondent credit institution;
- Approval from the Management of GARANTI BANK S.A. regarding the opening of the banking correspondent relationship.

The Bank shall not entered into correspondent relationship with financial institutions located in countries under international sanctions regime, and /or having direct relationship or being under the control of individuals/entities mentioned on international sanctions lists.

KYC&AML/CFT Training Program

Training programs shall include information related to the requirements in the legislation within the know your customer area, as well as the distinctive practical aspects, especially in order to enable the personnel recognize transactions suspected of being related to operations of money laundering and terrorism financing, as well as the taking of proper action.

The whole personnel shall be trained in order to make sure of the fact that they know their responsibilities, and keep them informed about the news within the area.

The main purpose of the training programs is to develop the skills of the employees of the Bank, promote high ethical and professional standards, and prevent the using of the Bank for carrying on criminal activities, or other activities that are against the law, and secure the carrying on of a banking activity in accordance with the requirements of the law.

The bank shall continuously ensure training programs within knowing your customer for the purpose of preventing money laundering and terrorism financing, so that the persons having responsibilities within such area are properly trained.

Archiving

All the records of reports (STR / ETR/CTR) sent to FIU and the related documents including any alert received on / or in direct relationship with customers and potential ML/FT from employees of the branches through whistle blower alert channel, must be kept for at least 5 years before being sent to the Bank's Archive, the term could be prolonged with no more than 5 years if there are details that such information could be requested by competent authorities.