PREVENTION OF MONEY LAUNDERING AND COMBATING TERRORISM FINANCING COMPLIANCE POLICY

April 2019

ZİRAAT KATILIM BANKASI A.Ş.
PREVENTION OF MONEY LAUNDERING AND COMBATING TERRORISM FINANCING COMPLIANCE POLICY

It is the policy of both Ziraat Katılım Bankası A.Ş. and its entire domestic and overseas branches and subsidiaries, which are carrying out their activities under Ziraat Finance Group, to prohibit and actively pursue the money laundering and any activities facilitating the laundering process, financing of terrorism or criminal activities.

It is essential for the overseas branches, subsidiaries and other affiliates of the Bank to comply and abide with this policy provided that it is not in contradiction with the applicable laws and regulations of their host country.

The Bank acts in compliance with the applicable laws and international standards on combating money laundering and terrorism financing. The Bank is determined to prevent the use of banking products and services for the purpose of money laundering and terrorism financing by ensuring full and absolute compliance of its management and employees with said legislation and standards.

This policy shall be reviewed on an annual basis and updated whenever required in order to ensure and maintain compliance with applicable legislation and international standards.

COMPLIANCE PROGRAM

The Bank has designated a Compliance Officer and established a Compliance Department consisting of employees who report to the Compliance Officer who is responsible for the conduct of compliance program in order to ensure that the Bank stays compliant with the applicable AML/CTF laws, regulations and other legislation. The Compliance Officer is entitled to demand and access all kinds of information and documents regarding its own area of duties from all units within the Bank in order to make a decision independently.

Compliance program has been established with a risk-based approach in order to ensure full compliance with the applicable laws and regulations and international standards in order to prevent money laundering and terrorism financing.

Compliance program includes designation of a compliance officer and establishment of a compliance department, implementation of policies and procedures, risk management activities, monitoring and control activities, conducting training and internal audit activities.

Risk management, monitoring and control activities under the scope of compliance program shall be carried out by the compliance officer under the supervision, inspection and responsibility of the board of directors, and the internal audit activities shall be carried out by the Bank's Board of Internal Auditors.

1. Risk Management

In line with the "Know Your Customer" principles in the bank, it is essential to identify the customers and those who carry out transactions on behalf of them in order to reveal the real beneficiaries of the transaction. It is prohibited to open anonymous or fictitious accounts and to conduct transactions with shell banks. Also, the relationship with customers who have been detected to use their accounts for money laundering and terrorism financing is terminated.

Where identification is not possible or no sufficient information can be obtained about the purpose of the transaction, business relationship shall not be established, and the requested transaction shall not be conducted. Business relationship shall be terminated when identification and identity verification cannot be completed where there is suspicion about the adequacy and accuracy of the client identification previously established.

In establishment of permanent business relationship, the Bank obtains information on the purpose and intended nature of the business relationship. In respect of other transactions, appropriate risk management system shall be established in order to adopt required measures to monitor risks under a risk-based approach.

Risk management activities include but are not limited to the following:

- Developing methods to identify, rate, classify and assess risks based on customer risk, product risk and geographic risk,
- Rating and classifying products, transactions and customers according to determined risk categories,
- Ensuring that risky customers, transactions or services are monitored, controlled and reported to warn the relevant units, and developing appropriate operational and control guidelines to ensure that the transactions are carried out with a senior's approval, and controlled when necessary,
- Questioning the consistency and effectiveness of risk identification and evaluation methods, risk rating and classification methods using case studies or retrospectively through real-life transactions; re-evaluating and updating such methods according to the conclusions arrived and the conditions that prevail,
- Conducting necessary improvement efforts taking into consideration the national legislation governing issues which involve risks as well as recommendations, principles, standards and guidelines introduced by international institutions,
- Reporting the results of risk monitoring and evaluation to the Board of Directors at regular intervals,
- Taking additional measures against high risk groups.

The Bank shall, to the extent possible, collect and record information about the purpose and nature of the transactions which do not seem to have a reasonable legal and economic purpose, particularly paying attention to the transactions to be conducted by and business relationships to be entered with real and legal persons in high-risk countries, organizations with no legal entity and the citizens of such countries.

The risks posed through money laundering and terrorist financing shall be identified, rated by the Bank and required measures shall be adopted to monitor, assess and mitigate such risks.

The Bank shall apply Enhanced Due Diligence measures for customers and transactions in high-risk categories. Enhanced due diligence measures may include:

a) Obtaining additional information about the client and updating the identity of the customer and actual beneficiary more frequently.
b) Obtaining additional information about the nature of the business relationship.
c) Obtaining information about the source of the assets underlying the transaction and of the funds owned by the customer as far as possible.
d) Obtaining information about the purpose of the transaction.
e) Ensuring that entering into business relationship, maintaining the current business relationship or conducting the transaction is subject to approval by a senior officer.
f) Increasing the number and frequency of controls implemented and strictly supervising the business relationship by means of identifying types of transactions which require additional control.
g) Making it mandatory that, in when establishing permanent business relationship, the first financial activity is conducted through another financial organization which implements the "Know Your Customer" principles.

In line with the Bank's international operations and its obligations arising from international banking legislation as a result of correspondent banking relationships, the Bank may choose to restrict the services offered and if necessary may terminate the business relationship if there are justified reasons to do so.

2. Monitoring and Control

The purpose of monitoring and control is to protect the Bank against risks and to monitor and control whether the Bank's operations are carried out in accordance with the Law and other regulations issued as per the Law as well as the Bank's policies and procedures on a permanent basis.

In the framework of monitoring and control activities, deficiencies discovered as a result of controls carried out to assure compliance with obligations are reported to the relevant units for necessary measures to be taken and the actions pursued. As part of monitoring and control activities, the Bank procures that the personnel carrying out these activities have access to internal information resources.

Monitoring and control activities include but are not limited to the following:

- Monitoring and controlling customers and transactions in high-risk group,
- Monitoring and controlling transactions with risky countries,
- Monitoring and controlling complex and unusual transactions,
- Controlling, through sampling method, whether the transactions exceeding a pre-determined limit are consistent with the customer profile,
- Monitoring and controlling linked transactions which, when handled together, are exceeding the limit requiring customer identification,

- Controlling, completing and updating the information and documents about the customer which have to be kept in electronic media or in writing and the compulsory information which have to be included in electronic transfer messages,
- Monitoring whether a transaction conducted by the customer is consistent with the information about the customer's business, risk profile and fund resources on a permanent basis throughout the term of the business relationship;
- Controlling transactions conducted by using systems which enable non-face-to-face transactions,
- Risk-based control of newly introduced products and services which may be misused due to technological developments.

Activities falling within this scope are executed by the Compliance Department. In carrying out the said activities, the Compliance Department may get support from the Bank's other departments when necessary.

The Bank shall pay particular attention to the transactions that are complex and unusual of size, with no reasonable legal and economic purpose, and obtain sufficient information about the purpose of the transaction, and retain the information, documents and records obtained in this scope for submitting to the authorities when required.

3. Training

The purpose of the Bank's training policy on AML/CTF is to ensure compliance with the Law and regulations, to develop a corporate culture by increasing the sense of responsibility of the personnel with respect to the Bank's policies, procedures and risk-based approaches and to update the personnel's knowledge.

The training activities related to the prevention of money laundering and terrorism financing will be carried out in accordance with the size, business volume and the changing conditions of the Bank.

Training activities will be carried out under the supervision and coordination of the Compliance Officer. It is essential to conduct the training activities under annual training program, prepared to cover the subjects given below. The training program will be prepared by the Compliance Officer with the contribution of the relevant units. The effective performance of the implementation will be supervised by the Compliance Officer.

Training activities will be reviewed according to scaling and evaluation results, with the participation of the relevant units, and repeated regularly.

In a manner to ensure training activities to be performed in the whole institution; training methods such as seminars and panels, creating workshops, use of visual and audio materials in training

activities, training programs supported by employee computers over internet, intranet or extranet will be used as much as possible.

The Bank shall provide all personnel with the necessary training about AML/CTF. Priority of in training is given to personnel who directly interact with the customer. The training of personnel who are in direct relation with customers shall be prioritized. It is essential that the newly recruited

personnel are trained during the orientation. Trainings shall be organized using in-class, on-the-job and remote training methods. In-class and on-the-job trainings shall be carried out by trainers determined by the Bank. It is mandatory to attend to remote training.

Trainings to be provided by the Bank to the personnel include but are not limited to the following subjects:

- The concepts of money laundering and terrorism financing,
- Stages and methods of money laundering and case studies,
- Legislation on AML/CTF
- Risk areas,
- Corporate policies and procedures,
- International legislations in prevention of money laundering and terrorism financing,
- Know Your Customer principles,
- Suspicious Transaction Reporting procedures,
- Obligation of retaining and submitting,
- Obligation of providing information and documents,
- Sanctions in violation of obligations

The activities falling within this scope are executed by the Compliance Department and the Training Department under the supervision and coordination of the Compliance Officer.

4. Internal Audit

The purpose of internal audit is to give assurance to the Board of Directors regarding the effectiveness and adequacy of the whole Compliance Program.The Bank procures that corporate policies and procedures are reviewed and inspected annually by using a risk-based approach in order to determine whether risk management, monitoring and control activities as well as training activities are adequate and effective, whether the risk policy is adequate and effective, and whether transactions are conducted in accordance with the Law and other arrangements issued as per the Law and the corporate policies and procedures.

Within the scope of internal audit activities;

- Defects, faults and abuses that are discovered during internal audits as well as opinions and recommendations to prevent their recurrence are reported to the Board of Directors.
- Deficiencies discovered in the course of monitoring and control studies and risky customers, services and transactions are included when determining the scope of the audit.

- When determining the units and transactions to be audited, it should be ensured that the quality and quantity of the transactions performed in the Bank is represented in fullest extent

Activities falling within this scope are executed by the Board of Internal Auditors.

REPORTING OF SUSPICIOUS TRANSACTIONS

In case there is any detection, information or suspicion of transactions conducted / attempted to be conducted with the Bank or through an agency of the Bank and is used for or related to money laundering and terrorism financing, investigations on these transactions are undertaken and transactions which are believed to be suspicious is reported to The Financial Intelligence Units within the periods and principles prescribed in the applicable laws and regulations. If there are documents or serious indicators found supporting that assets underlying the attempted transaction or the transaction being conducted are related to money laundering and terrorism financing, suspicious transaction is reported with a request to postpone the transaction along with applicable grounds and the transaction do not conducted for a period of time as specified in the regulation.

Due to the confidentiality of the suspicious transaction, any Bank personnel knowing that a suspicious transaction reporting is being made may not give information to anybody including the parties of the transaction, excluding examiners who are tasked with the supervision of obligations and the courts during legal proceedings.

SANCTIONS

Together with its domestic and overseas branches and subsidiaries, the Bank carries out its operations in accordance with the national legislation and international standards which govern the Bank's international operations. The Bank complies with international sanctions programs including particularly the sanctions of United Nations Security Council. The Bank shall not provide services to countries and activities subject to sanctions and shall not intermediate to any banking service in breach of sanctions.

The Bank shall not enter into business relations with persons and organizations that are listed in the sanctions list, shall not conduct transactions requested/ordered by such persons and organizations, and shall not intermediate transactions which directly or indirectly involve such persons and organizations. The Bank shall not open accounts for customers who are included in United Nations Security Council and other sanctions lists determined by the Bank. The Bank shall regularly scan the sanctions list in the event that existing customers who were not subject to sanctions previously may later be subject to sanctions. The Bank shall terminate its relationship with persons and organizations that are subsequently added in the sanctions lists.