AKTIF YATIRIM BANKASI A.S.

POLICY ON PREVENTION OF LAUNDERING PROCEEDS OF CRIME AND FINANCING OF TERRORISM

aktif bank

CONTEXT

AKTIF YATIRIM BANKASI A.S.

POLICY ON PREVENTION OF LAUNDERING PROCEEDS OF CRIME AND FINANCING OF TERRORISM

1. INTRODUCTION

The policy on Prevention of Laundering Proceeds of Crime and Financing of Terrorism of Aktif Yatirim Bankası A.S. (hereinafter referred to as the Bank) was developed in accordance with Law on Prevention of Money Laundering (hereinafter "Law") and related regulations regarding the implementation of that Law issued on 11.10.2006 by the Financial Crimes Investigation Board.

This Policy also takes into account the decisions and recommendations of international and specialized organizations, as well as business practice in the Bank›s relations with customers (including correspondent banks), including the principles and recommendations of the FATF and the leading practices of international financial institutions.

It has been prepared by taking into account the current regulations and best practices of the international finance sector, including but not limited to the following:

- Law No. 5549 on the Prevention of Laundering Proceeds of Crime
- Law No. 6415 on the Prevention of Financing of Terrorism
- Law No. 7262 on the Prevention of Financing the Proliferation of Weapons of Mass Destruction
- Financial Action Task Force (FATF) Recommendations and standards issued by the Wolfsberg Group on the prevention of money laundering.

2. DEFINITIONS AND ABBREVIATIONS

AML/CFT: Anti-money laundering and combating financing of terrorism (financing of proliferation of weapons of mass destruction, crimes such as bribery/corruption are also covered)

Beneficial Owner: Natural person(s) who ultimately control(s) or own(s) natural person who carry out a transaction within the Bank, or the natural persons, legal persons or unincorporated organizations on whose behalf a transaction is being conducted within the Bank.

Compliance Officer: The officer who is employed for the purpose of ensuring the compliance with obligations established through the Law No. 5549 on Prevention of Laundering Proceeds of Crime or the legislation issued on the basis of the Law and who is entrusted with the required authority.

Compliance Program: The integral package of the measures built in the Bank on the basis of the applicable Legislation and the Bank Policy to combat Financial Crimes

Deputy Compliance Officer: Bank's personnel who shall fulfill the conditions and qualifications required for the Compliance Officer for the conduct of the Compliance Program and shall work under the Compliance Officer to conduct the duties mentioned in the relevant Legislation

FATF: Financial Action Task Force

Financing of Terrorism: Providing or collecting funds for a terrorist or for terrorist organizations with the intention that they are used or knowing and willing that they are to be used, even without being linked to a specific act, in full or in part, in perpetration of the acts that are set forth as crime by the law.

Laundering of Proceeds of Crime (Laundering): Transactions whereby those earnings raised from unlawful means are injected into the financial system so as to convert them into non-cash form in particular to create the impression that they are derived from legal means, and to make them pass through a process in the financial system so as to conceal the illegal origins of the funds.

Legislation: The applicable law, regulations and communiqués as well as the decisions and orders by the MASAK to prevent Laundering of Proceeds of Crime and Financing of Terrorism.

MASAK: Mali Suçları Araştırma Kurulu (Financial Crime Investigation Board in Türkiye)

Permanent Business Relationship: Business relationship that is established between the Bank and its customers through services such as opening an account, lending loan, issuing credit cards, safe-deposit boxes, financing, factoring or financial leasing, life insurance and individual pension, and that is permanent due to its characteristics.

Politically Exposed Person: High-level real persons who are entrusted with a prominent public function by election or appointment domestically or in a foreign country and members of the board of directors, senior executives and other persons who have an equivalent duty of international organizations.

Suspicious Transaction: The case where there is any information, suspicion or reasonable grounds to suspect that the asset, which is subject to the transactions carried out or attempted to be carried out within or through the Bank, has been acquired through illegal ways or used for illegal purposes and is used, in this scope, for terrorist activities or by terrorist organizations, terrorists or those who finance terrorism.

Sanctions: Regulations aimed at comprehensively or non-comprehensively restricting or blocking the economic activities of the countries, individuals or entities to achieve economic and political goals.

Wolfsberg Group: Organization which is established by 13 global banks and which is aiming to develop standards for banks to combat Financial Crimes and Sanctions.

3. PURPOSE AND SCOPE OF THE POLICY

The purpose of Policy on The Prevention of Laundering Proceeds of Crime and Financing of Terrorism is;

- Implementation of Bank Compliance Program which is established with a risk based approach to ensure Bank's compliance with the obligations imposed by the Legislation, taking into account the international recommendations, standards, and best practices.
- Determining the strategies, controls and measures, processing rules, and responsibilities by evaluating the customers, transactions, and the services being provided with a risk based approach aiming to reduce and control the risks which the Bank can be exposed to, including the risk of losing reputation.
- To comply with the obligations regarding local regulations,
- The Bank's compliance with domestic and international sanctions,
- Ensure that the Bank employees are aware of the rules governing money laundering, terrorism and proliferation financing of weapons of mass destruction and to raise awareness and take responsibility for complying with them.
- Strengthening the corporate culture of the Bank's employees with regards to fight against Financial Crimes and Sanctions.

It is expected from financial subsidiaries, branches and representative offices of Bank, to take all necessary measures and to realize the necessary actions in order to comply with the Policy related with their activities.

The regulatory and supervisory agency that is authorized regarding AML/CFT/CPF is MASAK (Financial Crimes Investigation Board) organized under Ministry of Treasury and Finance. General principles required to be complied with in this regard and risks and penalties in case of violation of such obligations and strategies of struggle are set out in the laws in effects and related regulations, communiqués and guidelines.

Main legislations are listed below;

- Laws:
  - Law no. 5549 on Prevention of Laundering Proceeds of Crime
  - Law no. 6415 on the Prevention of the Financing of Terrorism
  - Law no. 7262 on the Prevention of the Financing of Proliferation of Weapons of Mass Destruction

- Article 282 of the Turkish Criminal Law No.5237

• Regulations:
  - Regulation on Measures Regarding Prevention of Laundering Proceeds of Crime and Financing of Terrorism
  - Regulation on Program of Compliance with Obligations of Anti-Money Laundering and Combating the Financing of Terrorism
  - Regulation on Postponement of Transactions Within the Scope of Prevention of Laundering Proceeds of Crime and Financing of Terrorism
  - Regulation on the Procedures and Principles Regarding the Implementation of Law on the Prevention of the Financing of Terrorism
  - Regulation on the Procedures and Principles Regarding the Implementation of the Law on the Prevention of the Proliferation Financing of Proliferation of Weapons of Mass Destruction

In addition to the local legislation, the Bank adopts recommendations, guidelines and standards published by international regulatory authorities and institutions listed below;

- Recommendations and Implementation Methodologies of FATF (Financial Action Task Force)
- Basel Principles (Know Your Customer Principles for Banks)
- EU Directives - UN Security Council Resolutions – OFAC Decisions
- Wolfsberg Principles.

The Bank will carry out assessments of the adequacy and effectiveness of current AML/CFT policy on an annual basis at least or whenever necessary.

4. MISSIONS, DUTIES AND RESPONSIBILITIES

The Bank's Board of Directors is ultimately responsible for ensuring that the Bank's AML/CFT obligations are met and effectively enforced.

Effective handling of the compliance program is performed by considering the three lines of defense. The units and departments which undertake risks and make decision are placed in the first line. Units and departments in this line are responsible for proper system development, process management and implementation of these systems and processes in accordance with policies and procedures established by the Compliance Department. The Group Internal Systems is placed in the second line of defense, within the framework of assigned duties and responsibilities. The Compliance Department within the Group Internal Systems is responsible for establishing policies and procedures with a risk-based approach, managing the ML/FT risks that the Bank may be exposed to, conducting monitoring and control activities and coordinating training activities. The third line of defense is the internal audit activity that checks whether the first and second lines of defense are meeting the risk management and control objectives.

AML/CFT/CPF are the main responsibility of all business units and employees of the Bank. It is obligatory for all of the Bank's employees in these defense lines to be aware of and appropriately act with this Policy and relevant procedures to protect the Bank against activities of money laundering and financing of terrorism.

Within the scope of Compliance Program, Board of Directors is authorized and responsible for;

- Ensuring the Bank's compliance with provisions regarding combating Financial Crimes,
- Approving the Policy, annual training programs and amendments to be made to these as per the developments,
- Assigning the Compliance Officer and Deputy Compliance Officer,
- Approving the charter for the Compliance Department governing the duties, powers and responsibilities of the Compliance Officer and Compliance Department
- Evaluating the results of risk management, monitoring, control, and internal audit activities and ensuring that the necessary measures have been taken,

- Ensuring that all activities are carried out in a coordinated and effective way.

Compliance Unit has been established and Group Head of Internal Systems has been assigned as Compliance Officer for ensuring compliance with obligations established with Law and regulations and communiques issued.

Compliance Officer who reports to the Audit Committee which is consist with two independent members of Board of Directors is assigned, authorized and responsible for;

- Undertaking those efforts in order to make sure that the Policy and Compliance Program is applied and pursue the necessary communication and coordination with the MASAK ,
- To evaluate the information and findings obtained through researches that he/she has carried out to the extent of his/her power and the possibilities regarding possibly suspicious transactions which were forwarded or detected by his/her initiative and to report the transactions which he/she considered to be suspicious to MASAK,
- To act bona fide in an objective and independent will, acceptable and honest manner in evaluation of suspicious transactions and reporting of them to MASAK, to take necessary measures for ensuring the confidence of reporting,
- To request all kinds of information and documents necessary from all units within obliged parties in the scope of evaluation of suspicious transactions,
- To carry out obliged party's training, research, development, observance, monitoring and control workings for ensuring compliance with obligations established with Law and regulations and communiques issued in accordance with Law and to provide necessary communication and coordination with MASAK,
- Establishing the Policy and submitting it to the Board of Directors for approval.

Compliance Officer may transfer some or all of its duties and authorities to the Deputy Compliance Officer in a clear and written way.

5. KNOW YOUR CUSTOMER PRINCIPLE

5.1 Know Your Customer Principles and Customer Acceptance

The first step in an effective AML/CFT program is the know-your-customer phase. Our Bank is obliged to know natural and legal persons in terms of social, financial and personal information. For this purpose, all necessary measures are taken to obtain all kinds of documents, especially regarding identity information and verify the accuracy of these documents. The Bank accordingly adopts a policy in line with the international standards and the applicable legislation and practices on know your customer principle.

Within the scope of ''Know Your Customer'' principles, business units and branches which establish business relationships with customers are responsible for ensuring that ID authentication and verification of customers and persons acting on behalf of the customers are carried out over documents and data obtained from independent sources, that necessary controls are implemented and measures are taken to identify the ultimate beneficial owners of transactions and that obtain information regarding the purpose and nature of the business relationship.

Under the "Know Your Customer" principle, necessary measures shall be adopted subject to the applicable legislation, and the Bank Policy and Procedures in order to:

- Verify the customer identity
- Take measures to confirm the beneficial owner
- Obtain satisfactory information about the purpose and nature of the requested transaction/process
- Performing risk assessment of customer during customer acceptance process and updating the risk assessment during the business relationship,
- Monitor the customer and transactions throughout the relations with customer and comparison of customer profile
- Monitor the high risk customers/transactions and other customers/transactions that require special attention.

In cases where identification cannot be done or sufficient information about the purpose of business relationship cannot be obtained, the Bank does not establish a business relationship or carry out the transactions of the related parties until the suspicion and deficiencies are overcome.

During the customer acceptance process, potential customers are subject to risk assessment and a risk score is created. Business relationships are not established with potential customers with prohibited risk levels. Enhanced due diligence is applied to customers in the high-risk category. Information and documents required to be obtained within the scope of risk assessment and KYC shall be kept up-to-date. The Bank regularly controls whether their customers are included in any international sanctions lists issued by UN, EU, UK, OFAC and other regulatory institutions.

Within the scope of this Policy, the Compliance Officer of the Bank and Compliance Department reporting the Compliance Officer are responsible for establishing a business flow regarding KYC principles to implement customer acceptance policy. Customer acceptance and whether to continue business relationship shall be determined within the scope of KYC principles.

5.2 Customer Identification and Verification

Customer identification shall be completed before the business relationship is established or the transaction is conducted. When establishing permanent business relationship, information on the purpose and intended nature of the business relationship shall be received. Customer identification process shall be conducted for below given cases;

- Regardless of the monetary amount when establishing permanent business relationships
- When the amount of a single transaction or the total amount of multiple linked transactions is equal to or more than one hundred and eighty five thousand (185.000) Turkish Lira
- When the amount of a single transaction or the total amount of multiple linked transactions is equal to or more than fifteen thousand (15.000) Turkish Lira in wire transfers
- Regardless of the monetary amount in cases requiring suspicious transactions reporting
- Regardless of the monetary amounts in cases where there is suspicion about the adequacy and the accuracy of previously acquired identification information

Customer identification shall be completed before the business relationship is established or the transaction is conducted. When establishing permanent business relationship, information on the purpose and intended nature of the business relationship shall be received.

The Bank shall retain documents, books and records, identification documents and records kept in all forms regarding their transactions and obligations for ten years starting from the last transaction date respectively and submit when requested.

5.2.1 Identification of Beneficial Owner

When establishing permanent business relationship with legal persons registered to trade registry, we identify the natural person partners holding more than twenty-five percent of the legal person's shares as the beneficial owner. ID authentication and verification of real persons who have 25% or more control or ownership shall also be made. For high-risk customers, this percentage may be reduced with the decision of the compliance officer. In case it is suspected that the natural person shareholder of the legal entity holding a twenty-five percent or more shares is not the beneficial owner or if the natural person having shares in this percentage does not exist, necessary measures are taken to reveal the natural person(s) who ultimately control the legal entity. The natural person(s) identified are considered to be the beneficial owner. When the beneficial owner is not identified the natural person or persons who are in the highest executive positions registered in the trade registry are considered the beneficial owners.

In cases where customer requesting the transaction declares that customer is acting for the benefit of someone else, the identity of the person requesting the transaction and the identity of the person for the benefit of whom the transaction is conducted shall be identified.

In cases where there is a suspicion that the person is acting in his/her own name but for the benefit of someone else although he/she has declared that he/she is not acting for the benefit of someone else, measures for the identification of the beneficial owner shall be applied.

5.2.2 Correspondent Relationships

Correspondent banks are classified among high-risk customers and may require EDD. Before establishing new correspondent relationships, approval shall be received from a senior manager. It has to be ensured that financial institutions have combat system against laundering and terrorist financing is appropriate and efficient via sending relevant questionnaires and information should be obtained from public resources on whether the financial institutions have gone through an inquiry related to laundering or terrorist financing and have been imposed a penalty; their field of business; reputation; and adequacy of audits performed in that bank. We use World Check database during account opening with correspondent banks. For existing correspondent bank client, if the client is high risk, we reviewed the AML related documents such as questionnaires, shareholder structure etc. on a yearly base, the other one time in 2 years. High risk transactions and customers (related clearing accounts) are subject to EDD. Senior Management and Compliance approvals have to be gained before account opening with correspondent banks. For transactions control; adverse media search is done for beneficiary and ordering customers and additional documents are requested in order to process transactions. The transactions of financial institutions are controlled monthly under the scope of our suspicious criteria. Our question set has to be filled for each suspicious transactions. And information and documents related to the suspicious transaction are obtained from the bank. In case of detecting any suspicious situation, termination process is started.

6. RISK MANAGEMENT

The purpose of the risk management is to ensure that necessary measures are taken to identify, rate, assess, and reduce risks associated with money laundering and terrorist financing that the Bank may be exposed. Depending on changing conditions, the risk management policy is regularly reviewed and updated, considering the legislation, recommendations, principles, standards and guides published by national and international institutions and organizations. The Bank evaluates alarms regarding risky transactions generated by scenarios to be defined in software products by using them to identify risky transactions. The Bank ensures that relevant units are informed to take necessary measures to minimize the risks identified as a result of such engagements. Enhanced measures are applied for high-risk customers and transactions. Acceptance of a customer classified as high risk requires approval from senior management within the scope of the risk-based approach.

Required to establish a risk profile of our customer in terms of money laundering and terrorist financing by considering the customer's profession, business history, financial status, accounts, commercial activities, resident country and the other relevant indicators, to identify high-risk customers, business relations and transactions, and to follow up them permanently, to keep up to date information, documents and records regarding the customer. The risk-based approach consists of three main risk types, taking into account the above criteria: customer risk, product/ service risk and country/region risk.

Customer risk: A vital step in a risk assessment is the analysis of the users of the products and services that Bank's offer. Abuse of our Bank by customer or persons acting on behalf of or for the account of customer for the purpose of money laundering or terrorist financing refers to Customer Risk. In assessing customer risk, the following criteria are taken into consideration, but are not limited to the following:

- Occupation and activity of customer,
- Establishment type of customers which are legal entities,
- Level of suitability and sufficiency of implementations for regulating and inspections with regards to combating Financial Crimes of the activity of the customer and/or the country and/or region, of which the customer is a citizen of and/or is residing and/or operating in,
- Duration of current banking relationship of customer with the Bank,
- The activity period of customers which are legal entities
- The type and nature of banking products and services being used by the customer,

- News about the customer being published in media with negative content (if any)

Product/ service risk: This risk type involves reviewing new and existing products and services offered by the bank to determine how they could be used to launder money or finance terrorism. The following products and services are monitored in the high risk category.

- Digital on-boarding
- Electronic transfers,
- Private banking products and services,
- Systems that allow non-face-to-face transactions,
- Products and services based on new and advancing technologies,
- Correspondent banking transactions,
- Businesses and transactions, the ultimate beneficiaries of which are not clearly and completely defined,
- Other products, services and types of transactions that are required to be given special attention in the concept of the risk management, monitoring and control activities included in the Compliance Program that is being carried out compliant with the international standards, domestic Legislation and this Policy,

Country/region risk: Countries that do not implement FATF recommendations or implement them incompletely and are therefore on FATF's high-risk and increased monitoring lists, countries where comprehensive sanctions/embargoes etc. are imposed by the UN, EU, OFAC, UK/OFSI and national authorities, countries and regions on drug production-distribution routes, countries and regions where crimes such as smuggling, terrorism, corruption and bribery are common, and tax havens/off-shore centers (offshore) constitute Country/Region Risk.

AML/CFT risk categories can be broken down into the following levels; Prohibited, High Risk , Medium Risk and Low Risk. Aktif Bank does not enter business relationship with Prohibited customer types. The transactions of current customers whose risk category turns to prohibited/unacceptable, are refused and the customer relationship termination process is initiated. Enhanced procedures are applied at the high-risk customers. Standard procedures are run for medium and low risk customers and transactions. Prohibited/unacceptable and high risk customer types and transactions are listed below.

Information and documents of existing customers obtained within the scope of KYC shall be regularly reviewed and updated. The update period shall be applied as follows according to the risk levels of the customers within the scope of money laundering and financing of terrorism;

- Once a year in high-risk customers,
- Once in two years in medium-level customers,
- Once in three years in low-level customers.

6.1 Prohibited/unacceptable customer and transaction types

Aktif Bank do not accept the following categories of customers;

- Customers who want to open with anonymous or fictitious names
- Customers who refuse to provide the required information and documentation
- Customers who are included in lists published by international institutions and organizations on the subject of laundering of crime income and terrorism (OFAC, EU, UN, HMT, etc.)
- In circumstances where identity verification not be undertaken or not receive sufficient information about the purpose of the business relation
- Customers who has a negative record in the bank's internal intelligence system for money-laundering, financing of terrorism, and financial crimes related thereto (fraud, counterfeiting, organized offenses, etc.)
- Shell banks
- Illegal bet, gambling transactions and any persons and entities involved in these sectors

- Persons and entities involved in drug trafficking and entertainment industry such as casinos, bar,
- Companies with bearer shares
- Arms, ammunition, gun etc. transactions,
- Any persons or entities involved in nuclear, atomic sector
- Persons and entities involved in payment system without licence

6.2 High risk customer and transaction types

On the basis of a risk based approach the following categories of customers identified as high-risk and may require enhance due diligence.

- Politically exposed persons (PEPs) and/or Politically Exposed Persons (PEP) is a Relevant Beneficial Owner of a Client
- Non-profit organizations (Associations, Foundations, Charities etc.)
- Off-shore/tax haven banks
- Correspondent banks
- Real or legal entities located in countries or region “non-cooperating countries and regions” as published by FATF and risky countries published by international organizations
- Non face-to-face transactions and customers who are accepted from non face-to-face channels.
- Exchange offices, precious mining sector
- Businesses dealing with high amounts of cash
- Defense industry, dealers and agents
- Customers with negative media news, cases and trials
- Notary, accountants, lawyers or other financial professionals holding accounts at a financial institution, acting on behalf of their clients
- Any persons and entities involved in cryptocurrency, digital money sectors and virtual currencies.

7. MONITORING AND CONTROL ACTIVITIES

The purpose of monitoring and control activities is to protect the Bank against risks and to monitor and control on a permanent basis whether the Bank’s operations are carried out in accordance with the Law and other arrangements issued as per the Law as well as the Bank’s policies and procedures. Monitoring and control activities are executed by the Compliance Department under responsibility of Compliance Officer. Results of monitoring and control actions are reported to Compliance Officer for evaluation in terms of suspicious transaction.

Monitoring and control activities are established and applied on a risk-based approach. In this respect, certain monitoring and control methods that suit the nature and level of risks associated with the Bank customers, transactions and services shall be developed and effectively implemented.

Monitoring and control activities are conducted by making necessary systemic arrangements and essentially taking into consideration the following issues:

- Monitoring and control of customers and transactions in the high-risk group
- Monitoring and control of complex and extraordinary transactions
- Monitoring and control of transactions conducted with high risk countries
- Controlling, through sampling method, whether the transactions exceeding a pre- determined limit by Bank’s risk-based approach are consistent with the customer profile
- Controlling, completing and updating the information and documents about the customer which have to be kept in writing and the obligatory information which have to be included in electronic transfer messages
- In money transfers made through the Bank within the limits set forth in the Regulation on Prevention of Laundering Proceeds of Crime and Financing of Terrorism, the Bank includes and verifies the following information on the sender: I. Full name, the title of the legal entity registered with the trade registry, the full name of other legal entities and

unincorporated entities,

II. Account number, and reference number related to the transaction in case the account number is not available,

III. Any of the following sender identification information as a minimum: address or place and date of birth or customer number, identity number, passport number, or tax identity number.

In money transfer messages, information on the recipient as specified in clauses (I) and (II) of this paragraph shall also be included. Verification of such information is not obligatory. Any incoming money transfer that does not contain the information in clauses (I), (II) and (III) shall be returned or the missing information shall be completed via the financial institution that sent this message. If the messages sent constantly contain incomplete information and such information is not completed when requested, the Bank shall consider rejecting money transfers from the sending financial institution or limiting transactions or terminating the business relationship with the said financial institution. No transfers shall take place to Anonymous Accounts

- 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-focused controlling of newly presented products and services that may become open to misuse due to developing technologies
- Controlling whether business relationship is established with individuals/institutions/ entities in blacklists of Competent Authorities within the scope of Prevention of Laundering of Proceeds of Crime and Financing of terrorism.
- Other monitoring and controls that may be necessary in this respect.
- Measures are taken to continuously monitor customers and transactions, taking into account Freezing of Asset decisions and potential matching criteria. In this context, the sender and receiver information in electronic transfer messages are also considered. In accordance with the Law on the Prevention of the Financing of Terrorism and the Law on the Prevention of the Financing of the Proliferation of Weapons of Mass Destruction, persons, institutions or organizations whose Assets are frozen and who have Assets in the Bank are monitored and if there is any increase in the frozen Assets, these increases are also subject to the Freezing of Asset provisions and reported to MASAK within the timeframes specified by the law.

The Bank uses systems to check whether existing or new customers are included in international sanctions lists in accordance with legal regulations. These systems enable a customer or transaction to be scanned in national or international sanctions lists. These sanctions lists include, but are not limited to;

- United Nations Security Council (UNSC),
- EU Consolidated Financial Sanctions List
- US – OFAC List,
- UK – OFSI Consolidated List
- Local sanctions lists (lists originally published/shared by MASAK, Ministry of Internal Affairs Terrorism Wanted List, etc.)
- A list of PEPs provided by a reputable commercial organization (such as World Check)
- Bank's internal watch list
- Sanction lists published under the Law No. 6415 on the Prevention of Financing of Terrorism
- Sanction lists published under the Law No. 7262 on Preventing the Proliferation of Financing Weapons of Mass Destruction.

Furthermore, existing customers are screened against the above sanctions lists whenever the lists are updated and to periodically screen their entire customer database against the lists

The Bank also uses these systems manually and automatically to identify suspicious customers and transactions, and to prevent the risks of money laundering and financing of terrorism. Scenarios that work to identify suspicious transactions are reviewed by the Compliance Department and, if necessary, enhanced due diligence is applied. If necessary, a suspicious transaction is reported following the approval of the compliance officer.

Central monitoring and control activities are carried out by the Compliance Department. To effectively implement the Compliance

Program in accordance with the applicable Legislation and the Policy and procedures at the Bank's Head Office and its branches, on-the-spot audit and control of the compliance of the transactions, are provided through internal audit and internal control activities. Results of the central monitoring and control activities as well as the data and information reported as a result of the internal audit and internal control activities are monitored and evaluated as a whole by the Compliance Department under the supervision of the Compliance Officer.

8. SUSPICIOUS TRANSACTION REPORTING

Where there is information or matters that would arise suspicions, indicating that a transaction which was or is to be executed by or through the Bank upon an application is associated or related with laundering of criminal proceeds or terrorism financing, necessary investigation to the extent permitted by the applicable means shall be carried out and any transaction concluded to be suspicious shall be reported to The Financial Crimes Investigation Board (MASAK) within such term and subject to such conditions defined in the applicable legislation.

Suspicious transactions shall be reported to MASAK regardless of the amounts.

Natural and legal persons, their compliance officers, legal representatives of the obliged parties, their managers and personnel complying with the obligation of reporting suspicious transaction, shall not be held responsible judicially and criminally in any way.

While fulfilling their tasks employees shall be alerted and act in accordance with legal obligations about identifying and reporting suspicious transactions against the following cases;

- Operations without any apparent legal and economical purpose
- Operations not related or not in proportion with the customer's occupation and income
- Transactions in which the customer is evasive or reluctant in providing the documents and information required by the obligations defined under law
- Transactions in which the customer is suspected of evading the reporting and record keeping procedures
- Transactions in which the customers give misleading and unverifiable information,
- Transactions related to credit requests the purpose of which is not economical and is not declared
- Transactions consisting of unusual transfers with large amounts to risky geographical regions and countries

All employees are made aware via training and briefings that they are personally obliged to report any suspicious activity or knowledge within the scope of AML/CFT and that failure to fulfill this obligation will have penal consequences. Branches, representation offices, agencies and / or affiliated units and Head Office units of the Bank cannot report suspicious transactions directly to MASAK.

Employees in the Bank shall report suspicious transactions via the related intranet system of the Bank to Compliance Department. The Compliance Department review the suspicious transaction notifications and reported to the Compliance Officer in order to be forwarded to MASAK. The Compliance Officer will review and evaluate the information contained in the Suspicious Transaction Reporting Forms sent to him by also considering the contents of the relevant applicable laws, regulations and communiques, and depending on the results of evaluation, will decide to or not to report the underlying transaction as a suspicious activity to MASAK The Compliance Officer will act in good faith, reasonably and honestly in the course of decision-making process. The Suspicious Transaction Reporting Forms decided not to be reported and transmitted will, together with the written grounds thereof, be kept and archived for a period of 8 years for submission to the official authorities if and when requested or deemed necessary.

It is obligatory to report the suspicious activities or transactions to MASAK within 10 (ten) workdays starting from the date when the suspicion occurred and immediately where delay is inconvenient.

In the event that new information and findings in relation to the reported transaction are obtained afterwards, another STR form shall be filled in and sent to MASAK without delay by stating that it is an additional report to the previous one.

Confidentiality is essential in the reporting of suspicious transactions. The Bank shall not disclose any information that the suspicious transaction has been or will be reported to anyone including the parties of the transaction, and the other organizations within the same financial group, except for the information provided for the examiners assigned for supervision of obligations and for the courts during trial.

All employees are prohibited from sharing confidential information within the scope of the relevant Law. In case of violation of these regulations, legal penalties are imposed and disciplinary measures are applied

8.1 Execution of Decisions on Freezing of Asset

MASAK is responsible for the execution of the decision on freezing of asset made in accordance with the provisions of the Law. The decision to freeze assets shall be notified to the Bank by MASAK using the appropriate technical communication tools to ensure that all accounts, rights and receivables are frozen. The said decisions shall be implemented by the Bank immediately upon receipt of the notification. If the Bank has any records of assets, it shall perform the required action and notify MASAK with information regarding the frozen assets within seven days from the date of notification. MASAK shall also notify the repealing decisions to the persons, organizations and institutions that's assets have been frozen. In case of any increase in assets, such increases shall also be subject to the provisions on freezing assets. The permission and authorization to access and dispose on frozen assets and the management of the relevant assets shall be administered pursuant to the relevant regulations of MASAK.

9. SANCTIONS

In addition to national legislation, as a minimum, the Bank shall ensure full compliance with the sanctions as announced by,

- United Nations Security Council (UNSC),
- EU Consolidated Financial Sanctions List
- US – OFAC List,
- UK – OFSI Consolidated List

Exceptionally and subject to the approval of the Compliance Department, the Bank may adhere to other sanction regimes in addition to the aforementioned. In that case, the sanctions lists to be considered are to be determined by the Compliance Department.

The Bank shall maintain and implement a compliance program to assess and address the sanction risks exposed by. The Bank does not get involved intentionally in any transaction designed to circumvent the sanctions.
The Bank oversees sanction risks at the customer onboarding, customer information update and executing customer transactions. In this regard,

- Customers and their shareholders, power of attorney holders and beneficial owners are screened against sanctions lists.
- Customer transactions to be carried with or through the Bank are screened to ensure they do not directly or indirectly involve Comprehensive Sanctions Target Countries/Regions and/or individuals or entities subject to sanctions.
- Until the review of the screening results is completed by the authorized personnel, customer onboarding and/or transactions are not concluded.
- Customers are periodically screened against the aforementioned sanction lists.

Persons, institutions and organizations published by the authorities listed above, which are completely prohibited from working or acting as an intermediary in their transactions, and persons and organizations owned or controlled by them or acting on their behalf are not accepted as customers. In the event that existing customers fall within this scope, the customer relationship is terminated immediately, without prejudice to national legal regulations.

10. INTERNAL AUDIT

The purpose of internal audit is to provide assurance to the Board of Directors regarding efficiency and sufficiency of whole compliance program.

The internal audit management is responsible to audit periodically on a risk sensitive basis whether the policies and procedures of the institution, risk management, monitoring and control activities and training activities are sufficient and efficient, the adequacy and effectiveness of the risk policy of the Bank, whether the transactions are carried out in accordance with the regulations and communiques issued in accordance with the Law and the Bank's policy and procedures.

Within the scope of internal audit activities;

- The deficiencies, mistakes and abuses determined as the result of internal audit, as well as the opinions and proposals for prevention of reappearance of them are reported to the Board of Directors.
- While determining the scope of control, the faults determined during the monitoring and controlling processes and the customers, services and transactions containing risk are included within the scope of control.
- While determining the units and transactions to be audited, it is ensured that units and transactions in quantity and quality that can represent all transactions carried out in the Bank are audited.

Deficiencies, errors and abuses revealed as a result of internal audit and opinions and suggestions to prevent their recurrence are reported to the Board of Directors by the Compliance Officer.

Relating to the works carried out in the scope of internal control activities; the statistics containing information regarding the annual business volume of obliged party, total number of staff and total number of branch office, agency and similar affiliated units, the number of branch office, agency and similar units which were controlled, the dates of controls carried out within these units, total control period, the number of staff employed during controls and the number of transactions controlled shall be reported to MASAK by compliance officer up to the end of March of every year.

11. TRAINING

Training of all employees about Financial Crimes and Sanctions and in regards to the legal obligations, Policy, procedures, and practices of the Bank are first step of improve corporate culture and awareness.

The purpose of training is ensuring compliance with obligations imposed by Law and the regulation and communiqués issued in accordance with Law, creating an institution culture by increasing the sense of responsibility of staff on policy and procedures of institution and on risk-based approach and updating of staff information.

Education programs are prepared by Compliance Unit and classroom trainings can be given by the Compliance Unit's staff. Training activities are organized by the coordination and cooperation of Compliance Unit and Education Unit. Training programs will be continuously reviewed and revised according to the current needs, and will be repeated annually so as to keep the knowledge of all relevant Bank personnel updated in line with their duties, obligations and liabilities

It is essential to train the new employees about the subject during the basic banking training period. The bank's existing personnel shall regularly be trained with classroom and e-learning methods.

The trainings to be given to staff by obliged parties shall at least cover the following subjects;

- Laundering proceeds of crime end terrorist financing
- The stages, methods of laundering proceeds of crime and case studies on this subject
- Legislation regarding prevention of laundering proceeds of crime and terrorist financing
- Risk areas

- Institutional policy and procedures
- In the framework of Law and related legislation
  - o Principles relating to customer identification
  - o Principles relating to suspicious transaction reporting
  - o Obligation of retaining and submitting
  - o Obligation of providing information and documents
  - o Sanctions to be implemented in violation of obligations

- The international regulations on combating laundering and terrorist financing

Necessary information and statistical data in relation to the training courses in progress regularly keeping subject to the applicable legislation, and shall report through Compliance Officer to MASAK at such times and in such manner to be defined.

12. RECORD KEEPING

Within the scope of the laws on AML/CFT, the Bank is obliged to keep for eight years the documents related to the customer accounts and transactions regarding the obligations in the relevant Laws and transactions from the date of issuance; books and records from the last registration date; and ID authentication documents from the last transaction date and to present it to the authorities if requested.

Documents and records of suspicious transactions reports made to MASAK or internal reports made to the compliance officer, documents attached to reports, the written reasons relating to suspicious transactions decided not to be reported by compliance officers are all in the scope of obligation of retaining and submitting.

The Bank shall keep the records related to customer accounts and transactions for at least 10 years pursuant to the Banking Law and relevant regulations.

13. PROVIDING INFORMATION AND DOCUMENTS

All kinds of information, documents and records on all kinds of media, including microfilms, magnetic tapes, diskettes, CDs and similar media requested by MASAK or auditors, as well as all information and passwords required to access these records or to make them readable, must be provided in full and accurately in the requested manner, form and time without delay and the necessary facilities must be provided.

14. EFFECTIVENESS

Compliance Officer is responsible to the Board of Directors for implementing this policy.

The Policy becomes effective on the date it is approved by the Board of Directors.

The Policy is reviewed at least once in a year with the aim to ensure compliance with the regulations and international standards and updates, whenever required, are submitted for the approval of Board of Directors.

Any amendments or updates that may be realized in relation to the Policy later on are also enforced with the approval of the Board of Directors.