BANKPOZITIF KREDI VE KALKINMA BANKASI A.S.

COMPLIANCE RISK POLICY

The basis of the banking business is trust, reputation and stability. The banks constituting the Turkish banking industry have established the Banking Code of Ethics that has also been approved by the Bankpozitif Board of Directors to implement among each other and in all kinds of businesses and transactions with their customers and employees as well as other organizations. "Combating Laundering of Criminal Proceeds and Financing of Terrorism" is one of the main ethical values governing the performance of banking operations such as "Honesty", "Impartiality", "Reliability", "Transparency", "Observing Social Benefits and Respecting the Environment." BankPozitif has adopted, in this context, the prevention of laundering of proceeds of crime and terrorist financing as one of its fundamental priorities and aimed at ensuring full compliance with this and legal regulations on the matter.

The compliance risk and, in particular, money laundering and terrorist financing risk is a risk area that Bankpozitif employees at all levels constantly consider during their work. The management of the risks related to money laundering and terrorist financing is coordinated by the Compliance Department. In addition, the duties and responsibilities of the departments concerned in the management of these risks have also been specified in the relevant written regulations.

The Bank staff at all levels are charged with and responsible for:

- Learning and complying with the compliance regulations within the framework of their areas of duties and responsibilities, particularly the Law no. 5549 on the Prevention of Laundering of Proceeds of Crime and related legal legislation and all of the bank's internal regulations related to this issue.
- Attending the training activities to be held by the Bank for managing the compliance risk.

The Risk Management Program

Bankpozitif has identified a risk management program on the issue of complying with the obligations relating to the prevention of laundering and terrorist financing. This program has been described primarily in the Compliance Risk Policy determined by the Bankpozitif Board of Directors as well as in the internal regulations issued by the relevant departments within the framework of their mandates. The Risk Management Program including the basic policies and practices relating to managing the Bank's risk for laundering and terrorist financing are summarized below.

The Risk Management Program contains customer acceptance policy, rules for customer due diligence process, monitoring and control applications, training and audit processes that have been determined by a risk-based approach.

Customer Acceptance Policy

As a basic principle, Bankpozitif does not provide banking services to individuals and institutions that have not gone through know your customer stages.

Accounts are not opened to persons who refuse to provide the information and documents that must be submitted in accordance with legal regulations. On the other hand, avoiding from submission of the information and documents that must be obtained pursuant to the bank's internal policies and processes also constitutes reasonable grounds for the rejection of the demands to open accounts or to make transactions in the case of existing customers.

The Bank does not accept the following people and organizations as a customer:

- Persons whose true identities and addresses cannot be identified
- The persons and Institutions mentioned in the blacklists issued by official bodies on the laundering of criminal proceeds and terrorism (OFAC, EU, UN, and the like.)
- Banks and institutions without a physical address
- Individuals and institutions carrying out gambling activities, including those operated via the Internet
- Individuals and institutions not submitting the information and documents to be requested by the Bank within the scope of FATCA, CRS and other similar tax regulations, non-financial institutions that are not participants within the scope of FATCA, and customers determined to be noncompliant
- Depending on the country of residency, foreign residents that do not submit the documents or declarations demanded by the Bank concerning tax liability
- Those whose account opening requests had been refused by other banks due to regulatory reasons including the tax regulations
- Those who trade in bitcoin or other similar virtual currencies on behalf of others

The Bank does not perform customer identification by nicknames or names consisting of a number.

The acceptance as a customer of the companies with bearer shares or shares that can be converted into bearer shares and the companies whose articles of association contains a provision that the company could issue bearer shares is subject to special processes of approval.

Avoidance by the customers from submitting the information and documents that must be submitted pursuant to legal regulations and tax regulations or from signing the documents required constitutes reasonable grounds for the rejection of the demand to have an account opened for the customer. The Bank also does not establish permanent business relationship or perform the transaction that was requested in cases where it could not obtain adequate information regarding the purpose of the business relationship or the transaction that was requested to be realized pursuant to the existing legal regulations, or when the customer refrained from meeting the demands for information in this direction.

The Compliance Officer may request, at his own discretion, the closure of an outstanding account or the refusal of the request for a new account to be opened when he deemed necessary because of the risks for laundering of criminal proceeds and terrorist financing.

The Bank saves in the database for negative records the persons that it did not accept or decided to terminate the relationship with because of such issues.

Maximum attention and care is taken in accepting as customers the individuals and institutions with the suspicion as to the legality of the acquisition of their wealth and funds and the persons with negative social reputation (named in criminal activities such as environmental pollution, bribery, corruption, and smuggling.)

The Bank does not allow the utilization of hold-mail addresses (meaning the addresses kept at the organizations that provide this service at which the emails sent temporarily to persons are kept on behalf of the owner of the address without being returned to the sender) or poste restante addresses (cases where a post office branch is stated as the address information) as the sole address information by its customers.

Customer Recognition

The principle of customer recognition reduces and controls the risk of money laundering and facilitates the identification of transactions linked to illegal activities. The aim of the customer's recognition is to ensure the clarity of the customer's transactions and information and to establish and maintain a relationship based on mutual confidence.

Before any banking services are offered to the customers, the nature of the transaction to be carried out and whether the transaction is reasonable accordingly are evaluated. It is required during an account opening process that the structure of account ownership be determined and that the relationships among the people who are parties to the account be revealed.

The Bank deals with the customer recognition process by a risk-based approach. The risk model determined by the Bank is also used in the monitoring and control of customer transactions.

Within the scope of know your customer process, information is obtained towards the customer's recognition from the customers that would be provided with an account at the Bank. The scope of the information to be obtained is determined according to the type of customer and the expected account activity. Such information may be obtained through digital customer information forms or forms with a similar name, credit application forms, customer documents, or interviews with customers. Such information is confirmed by documents or independent sources when necessary and feasible.

Acquisition of information is intended on the following topics under the KYC process:

- Purpose of opening an account,
- In the case of customers residing abroad, why was an account needed to be opened in a foreign country,
- Whether the person has the political influence and, if a politically influential person, details of the position he has and whether he obtained his wealth when holding such a position,
- Customer’s profession, the main business line that earns income, the source of his wealth
- Customer’s transaction profile and capacity
- Workplace or place of activity
- Whether his requests for opening an account at another bank have been rejected due to legal reasons
- In company accounts; the company's field of activity, its main customers and suppliers

The correct and complete fulfilment of the transactions towards the customer's recognition is of great importance with respect to accurate assessment of the customer within the framework of the bank's customer acceptance policy.

The enhanced know-your-customer rules are applied for the customers that are determined to be of high risk because of the risk assessment to be made by the Bank.

During the continuation of the active relationship with the customer, the Bank carries out regular review, monitoring, and control activities to make sure that the transactions that occur on account in a continual manner comply with the information that the Bank has relating to the customer and the source of the wealth.

Identification

It is the most important step in the customer recognition process. The Bank undertakes the customer identification in transactions that requires identification within the framework of the legislation determined by MASAK and confirms the information within the scope of identification again by the identity documents defined in the legislation.

The customer relationship cannot be established before the obligations relating to the identification are fulfilled pursuant to the legal regulations. Identification is not an obligation limited to the customers only, but also covers other people and institutions such as real beneficiaries, persons authorized to represent whose identification has been mentioned in the MASAK legislation as required. In the establishment of permanent business relationship, the necessary measures are taken by the Bank relating to the issue of determining the actual beneficiaries, including obtaining statements on the issue from the customers pursuant to the relevant legislation and identification is carried out for such individuals as well and saved in the banking system.

For the establishment of permanent business relationship with individuals residing abroad, customers are expected to provide the statements, information, and documents to be requested by the Bank concerning tax liabilities. No accounts are opened for the individuals acting on behalf of / in favour of a third person that fail to present the information and documents demanded by the Bank regarding such an individual.

In cases allowed by the MASAK legislation, the Bank may implement simplified measures towards the identification and monitoring of the customer transactions.

Except for the cases allowed in legal regulations, the identification is to be made face-to-face by a bank employee or the bank's contracted representative (support service firms.)

The Bank takes the necessary measures in order for the appropriate and sufficient identification to be carried out for the individuals that benefit from the services in which innovative technological tools are used.

The business relationship with the customer is not established in case of avoidance of the customer from providing the information, documents and declarations that the Bank must get pursuant to the legal regulations that it is subject to, including the fight against money laundering and terrorist financing and tax regulations as well. The same obligation also applies to transactions that existing customers want to perform during the business relationship. The realization of the transaction that was requested may be denied in cases where the transaction that the customer wanted to realize was not fully clear, where the customer refrained from making an explanation on this issue, or where, even if an explanation was made, it was not deemed by the Bank to be satisfactory / adequate.

Customer Review Process

Customer recognition is not a process carried out and completed at once and the information related to the customer should be kept up-to-date as long as the customer relationship continued. This can be ensured only through a regular review of the assessments made within the scope of the principle of know-your-customer, and the determination and completion of the shortfalls, if any. In order to increase efficiency in this issue, a risk-based approach is exhibited in determining the need for revision as well, as was the case in customer acceptance. More stringent control procedures are implemented within the scope of this approach towards the customers of high risk.

The Bank takes, within the framework of legal regulations, the measures that would guarantee the provision of the information and documents that are required to be obtained from the customers relating to account opening, and establishes the control mechanisms that are required for this purpose. In the event of the identification / emergence of such a deficiency later on, the deficiencies in question are required to be completed in a way and within a period that would not be in contravention of the provisions mentioned in legal regulations.

On the other hand, identification and verification are conducted again regarding an existing customer in case of doubt about the adequacy and accuracy of the customer's ID information. The business relationship is terminated within the framework of the legislation in cases where this cannot be done.

Change of ownership of control or field of activity in legal entities, significant changes in senior management or the structure of activity, change in the real beneficiaries and significant changes in the customer's transaction profile activate the review process.

Determination of true / ultimate beneficiary

The Bank takes the measures set out in the legal legislation in order to determine whether the action has been taken on account of someone else in customer acceptance and in transactions requiring identification that are realized before or through the bank.

In the process of determining the actual beneficiary, the real person or persons holding the ultimate control over the legal entity within the framework of the legislation are expected to be uncovered while customer acceptance is made for legal entities registered in the trade register.

When required, the real person or persons registered in the trade register with the highest level of executive authority are considered as the real beneficiary in the capacity of senior executive. The same principles apply in determining the final beneficiary in other entities and unincorporated entities as well.

The practices for the determination of the actual beneficiary are repeated within the scope of the customer review processes.

Customer Risk Classification

The Bank subjects the individuals and organizations that it will accept as customers, to an evaluation in terms of various risk factors with respect to laundering and terrorist financing risks. As a result of these evaluations, enhanced measures are implemented in the processes for customer acceptance and monitoring of the transactions for customers that have been identified as being at a higher risk level.

The customer risk classification system is essentially based on country risk, customer risk and product risk factors. Apart from these main risk factors, any risk indicators related with a customer is reflected to the risk level. The Bank also uses transaction profile of a customer, which is determined based on the conducted transactions of a customer, as a risk factors in its classification model.

The following specific risk situations are also taken into account by the bank in the risk scoring system.

- Politically exposed persons
- Companies with bearer shares or companies with shares that can be converted into bearer shares
- Customers residing or operating in high-risk countries (companies not set up in a high-risk country and sustaining their activities in high-risk countries included)
- Associations and foundations
- Casinos and other gambling businesses
- Offshore financial institutions
- Monetary service providers

More stringent risk management and control activities are implemented for the specific cases mentioned above as well as the customers that have been considered to be of high risk because of the risk scoring.

The bank reviews at regular intervals the risk scoring and classification model that it has been using.

Monitoring and Control Practices

The Bank's monitoring and control practices towards the prevention of money laundering and terrorist financing includes such practices as determination of the risky transaction and product groups and implementation of additional measures for such groups, identification of suspicious transactions, prevention of transactions that may be associated with terrorist financing, keeping secrets, and storage of the information and documents.

Risky Operations and Products

Certain products and operations may vary compared to other products and services in terms of laundering and terrorist financing risk. In this context, the Bank considers the following transactions and products more risky and implements risk management measures that are specific to them.

- Transactions Conducted with Risky Countries
- Correspondent Banking
- Transactions in Return for Cash
- Transactions in Cash and Quasi Cash
- Electronic Transfers
- Check Transactions
- Technological Channels, Internet, Call Center Operations
- Transactions conducted in the accounts of high-risk customers
- Transactions of private capital funds, venture capital funds and hedge funds

- Transactions conducted in other special nature accounts (Extraordinary transactions conducted in the accounts of children or elderly customers, custody accunts etc.)

New Products and Activities

New products or activities that the Bank has planned to provide or to start must be evaluated in terms of the laundering and terrorist financing risks. In this context, they are assessed by the Compliance Officer with respect to the laundering and terrorist financing risks prior to the approval of the product / activity. The bank takes the necessary measures in order for an appropriate and sufficient identification to be made for persons benefiting from the services in which innovative technological tools are used.

Reporting System for Suspicious Transactions

The Bank monitors customer accounts regularly in order to identify suspicious circumstances in customer transactions. In this monitoring process, the issue of whether the customer's transactions are compatible with the customer profile and transaction profile known to the bank is evaluated.

All employees of the Bank are obliged to notify suspicious situations to the Compliance Officer in the event that they noticed suspicious situations in transactions, which they were involved in, that were conducted or attempted to be conducted before or through our bank.

The notification of suspicious transactions is required to be made as soon as possible and within the time specified in the regulations at the latest. In cases where delay is not desired, a notification is made as soon as possible by the Compliance Officer to the Office of Public Prosecutor that is in charge and competent, apart from the notification to be made to MASAK.

Suspicious transactions require by definition a subjective assessment to be made regarding the transaction. Therefore, bank employees need to know the types of suspicious transactions towards laundering and terrorist financing. The Bank gives regular trainings to its employees and measure their knowledge, for this purpose.

The Bank takes the types of suspicious transactions established by MASAK as the basis on the issue of identifying suspicious transactions. However, it takes into account that those types of transactions are exemplary and suspicious transactions other than those may be encountered.

In cases of monitoring customer transaction against suspicious transactions, the Bank uses software that has been prepared for this purpose. However, manual controls are established when necessary.

Prevention of Transactions Connected with Terrorist Financing

The Bank benefits from technological solutions in order to determine the transactions that may be associated with terrorist financing.

The phonetic matching logic is used to control customer transactions through sanctions lists such as OFAC, EU, and UN.

The Bank closes the accounts identified in retrospective controls as having made transfers to terrorist organizations, by observing legal regulations as well.

Obligation to Provide Information and Documentation

The Bank is obliged to provide completely and accurately, and to ensure the necessary facilities for, all kinds of information and documents to be requested by MASAK within the scope of its obligations to prevent laundering of criminal proceeds and terrorist financing as well as the records in any media related thereto, all necessary information and passwords that are required to provide access to these records or make them readable.

Confidentiality Obligation

Bankpozitif employees cannot disclose and use for the benefit of themselves and third parties the secrets or other issues which must be kept confidential that they have learned, due to their tasks, relating to the individuality, transactions and account status, businesses, undertakings, wealth or occupations of the customers and the individuals related to the customers, except for the persons and institutions expressly authorized in law.

The suspicious transaction notification that has been made cannot be disclosed to anyone, including those who are parties to the transaction, except for the audit staff conducting the liability audit and the courts during a trial. Such obligations continue even after the Bankpozitif employees resigned their offices.

Storage of Records and Documents

The documents in any media related to the obligations and transactions that have been imposed by the Law on the Prevention of Laundering Proceeds of Crime are retained for 8 years from the date of issue, the books and records are retained for 8 years from the date of last record, and documents related to the identification are retained for 8 years from the date of last transaction. The rules for longer retention periods arising from other legislation are reserved.

Combating Corruption

The Bank has adopted as the basic principle to fulfil its activities with highest ethical values and in full compliance with the legal regulations for the prevention of corruption. In this context, the Bank aims at preventing the use by the customers of their accounts at the Bank in the realization of the transactions associated with corruption. Therefore, the Bank takes measures to identify suspicious transactions that may be related to corruption. The Bank considers itself in this context committed to the international standards and FATF principles on the issue besides the legal regulations on combating corruption.

The Bank displays a tough stance in the fight against corruption. This stance is applicable with regard to both actions by its employees and customer transactions. With respect to actions by the employees, none of the bank employees can obtain benefits, within the scope of their duties at the Bank, from the customers, suppliers or service providers or other third parties that they have a relationship with, excluding the symbolic gifts (other than money) that can be accepted by the approval of the manager. The employees are obliged to notify to their managers the offers made to them concerning the provision of gifts or benefits that have been excluded from the scope of the exception mentioned in this article. The Bank shall not provide any gift, benefit or privilege to public servants or employees of the institutions in the nature of public agency, even if they are not government agencies. The principles for the implementation of this policy rules are determined by the Internal Control and Compliance Group in appropriate sub-regulations.

The Bank determines the key risks, risky sectors and possible transaction profiles against the corruption risk that may arise due to customer transactions and ensures required controls are implemented during the operations of the Bank.

The Bank establishes control processes needed in order to determine if the customers, control owners or final beneficiaries in corporate accounts are PEP or not. Such controls are repeated as part of periodic customer review processes.

In cases where opening an account for a foreign person with political clout is in question, the Bank act more carefully and cautiously as to the goal of account opening and the source of funds coming into the account. That the customer is from a country known for its widespread corruption is considered by the Bank to be a case that especially increases the level of risk.

The Bank accepts executives of the international organizations as well as PEP. Within this scope, when assessing the relevant risks, the seniority of the position, the length of time since the end of his service, as well as the connection between the position he held and his current occupation are taken into consideration by the Bank.

Compliance with Tax Regulations

In line with the Bank's goal of full compliance with legal regulations, only the money declared to tax authorities are accepted to customer accounts. The Bank deems itself to be obligated to avoid situations in which it receives money which is not declared to the tax authorities.

The Bank receives when needed a declaration from its customers as to whether they have tax liability in other countries or the monies owned by them are reported to the tax authorities in their home country or not.

Acceptance of a fund into an account will be avoided in the case of a suspicion arises concerning that the fund is a declared fund and the economic reasoning and the purpose of the transaction could not be explained by the client in a reasonable and sufficient manner supported with documents when needed. If the clients avoid from providing information or documents demanded by the Bank or they cannot bring a reasonable explanation, the Bank avoids performing the requested transaction and consider terminating the customer relationship.

Bank staff cannot provide any advice and guidance to the customers with regard to the personal taxation issues of their customers.

Training

Educating the Bank's staff about the risks on the issue of money laundering and terrorist financing as well as the liabilities related to them, and keeping the information about them up-to-date are mandatory. The staff, particularly those who directly carry out customer acceptance transactions or those who have higher risk of encountering suspicious transactions, receive trainings at regular intervals and take examination.

The training is configured to include at least the minimum topics mentioned in the legal regulations as well as the bank's practices relating to the issue.

The level of knowledge about the subject of the Bank's staff is measured regularly with a test application to be held every year. The personnel with scores below the specified threshold grade are provided with retraining.

The Bank shall determine the training needs of its staff concerning the combating corruption, compliance with tax regulations and other matters regulated in the Compliance Risk Policy and gives regular trainings either as part of AML trainings or as separate trainings.

Auditing

The implementation of the compliance program with respect to the obligations for the prevention of laundering of criminal proceeds and terrorist financing is audited regularly by the Internal Audit Department of the Bank with a risk-based approach. The issues related to the scope and frequency of the audit, the audit method to be followed, and the reporting are performed and reported in accordance with the existing regulations and procedures of the Internal Audit Department.

The Compliance Officer assesses, by examining other audit reports of the Internal Audit, if there was a hitch in terms of the matters covered by this policy and takes preventive / corrective measures, if necessary. For this purpose, the Compliance Officier and other concerned departments works closely with the Internal Audit Department of the Bank.