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

06-01-POL-003

February / 2018

Alternatif Bank

Table of Contents

Alternatif Bank

I. INTRODUCTION

1. OBJECTIVE

To ensure the compliance to the Law No.5549 on Prevention of Laundering Proceeds of Crime and to the Law No.6415 on the Prevention of the Financing of Terrorism and to the obligations on prevention of money laundering and terrorism financing which were put into effect on the basis of such mentioned Laws, to enable the assessment of customers, transactions and presented services with a risk-based approach, to develop strategies, operational rules and responsibilities for the purpose of mitigating risks to be exposed to within this scope, to raise the awareness of our employees in this respect and to prevent the risks which our Bank and employees may be exposed to with the help of the constituted policy and procedures

2. SCOPE

Head Office and Branches

3. DEFINITIONS

Below given abbreviations used in this procedure mean below given definitions;

Abbreviation	Meaning
The Bank	Alternatifbank A.Ş. (Alternatif Bank)
The Law	The Law No.5549 on Prevention of Laundering of the Proceeds of Crime which was published in Official Gazette No. 26323 dated 18.10.2006
The Law on Prevention of Terrorism Financing	The Law No. 6415 on the Prevention of the Financing of Terrorism which was published in Official Gazette No.28561 dated 16.02.2013
Regulation on Measures	Regulation on Measures Regarding Prevention of Laundering Proceeds of Crime and Financing of Terrorism which was published in Official Gazette No. 26751 dated 09.01.2008
Regulation on Compliance	Regulation On Program of Compliance with Obligations of Anti-Money Laundering and Combating the Financing of Terrorism which was published in Official Gazette No.26999 dated 16.09.2008
FCIB (MASAK)	The Financial Crimes Investigation Board of Ministry of Finance, Republic of Turkey
Legislation	The applicable Law, Regulation and Communiques as well as the resolutions and orders of FCIB on prevention of laundering proceeds of crimes and financing of terrorism
Laundering Proceeds of Crime (Laundering)	Transactions for converting the earnings gained through illegal methods into non-cash form by

	injecting them into the financial system and legitimizing such illegal earnings by means of changing their illegal origins by making them pass through a process in the financial system, with the purpose of creating the impression that such illegal earnings are raised through legal means
Terrorism financing	To obtain or collect the money or all kinds of goods, rights, receivables, income and benefits, whose value could be represented with money, as well as the benefit and value occurred as a result of converting all these into one another, with an awareness and intention of all these to be utilized wholly or partially for the purpose of committing terror crimes
Permanent Business Relationship	means a business relationship that is established between obliged parties and their 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
Suspicious Transaction	The transaction which contains any kind of information, suspicion or issue raising suspicion about the fact that the assets which are the subject of the transaction performed or attempted to be performed at the Bank or via the Bank have been obtained through illegal methods or utilized by the terror organizations, terrorists or parties financing terrorism or have relevance or connection with thereof,
Compliance Officer	Bank personnel who is appointed as per the Law on Prevention of Laundering Proceeds of Crime and the legislation which has been put into effect on the basis of the Law and is obliged and authorized to ensure the compliance of the Bank to the obligations arising from the mentioned legislation
FATF	The Financial Action Task Force (FATF) is an inter-governmental body whose purpose is the development and promotion of policies, both at national and international levels, to combat ML and FT. Consistent with its mandate, the priority of the FATF is to ensure global action to combat ML and FT and concrete implementation of its 40+9 recommendations throughout the world. Starting with its own members, the FATF monitors countries' progress in implementing AML/CFT measures, reviews the techniques and counter-measures, and promotes the adoption and implementation of the FATF recommendations globally.

AML	Anti-Money Laundering
CFT	Combating the Financing of Terrorism
FI	Alternatif Bank's Financial Institutions Department
Off-Shore Bank	An offshore bank is a bank located outside the country of residence of the depositor, typically in a low-tax jurisdiction (or tax haven) that provides financial and legal advantages, such as greater privacy, little or no taxation (i.e. tax havens),easy access to deposits , protection against local, political, or financial instability
Beneficial Owner	Beneficial owner means natural persons who carry out a transaction within an obliged party, and natural person(s) who control(s) the natural persons, legal persons or unincorporated organizations on behalf of whom a transaction is conducted within an obliged party or who is the ultimate owner of the transaction or the account belonging to them

4. REGULATORY COMPLIANCE

This Policies Manual is prepared taking into consideration laws and regulations set in the State of Turkey, including instructions issued by the The Financial Crimes Investigation Board (FCIB) In the event that a conflict exists between this Manual and regulatory pronouncements, the latter shall take precedence. Amendments to this Manual shall then be required to ensure compliance. Moreover, ABank shall ensure that it is in compliance with applicable laws and regulations of the countries that it operates in, and if any such conflicts arise, the Legal and Compliance Departments should be consulted.

5. POLICIES SUMMARIES

This Manual provides guidance as follows:

Risk Management

The purpose of risk management policy to enable the definition, grading, monitoring, assessment and mitigation of financial, reputational and operational risks which our Bank or employees could expose due to such reasons as benefiting of the services presented by our Bank with the purpose of laundering proceeds of crime and financing terrorism or non-compliance with the Law and regulation and communiques issued as per the Law and to define the measures within Bank which will be implemented for the principals of customer due diligence at minimum level.

Monitoring and Control Activities
Monitoring and control activities, carried out in the bank in the context of Prevention of Money Laundering of Criminal Proceeds and Terrorism Financing, is defined in this policy.

The purpose of monitoring and controlling is to protect the Bank against the risk and continuously monitor and control whether or not the Bank activities are being conducted in line with the Law, regulation and communiques, internal policy and procedures.

Suspicious Transaction Reporting
This policy describes how the reporting of suspicious transactions should be done. It is referred to the confidentiality of suspicious transaction reports and the procedures and practices to be followed.

Compliance Officer
This Policy discusses the appointment, roles/responsibilities and resignation of the Compliance Officer.

Internal Audit
This Policy describes the importance of audit reviews in relation to AML/CFT.

Training Policy
This policy discusses the ongoing AML/CFT training programs necessary for all Alternatif Bank officers and employees.

Documents, Record Keeping and Retention
This Policy provides guidelines on the maintenance of a complete, standardised and secure record of transactions and trainings in relation to AML/CFT.

Corporate Procedures
This Policy describes the detailed issues such as the persons who are responsible from the all measures and operating rules defined in the scope of this Compliance Policy, who or which departments will be responsible from the approval, performing, reporting and monitoring of the transactions as per the specific risk limits will be defined with the sub-regulations which are issued or to be issued with the names of procedure, instruction, form and list.

Authority And Responsibility
Conducting the compliance policy effectively is under the ultimate responsibility of the Board of Directors.

II. POLICIES

1. RISK MANAGEMENT

In the Article 11 of the Regulation on Program of Compliance with Obligations of Anti-Money Laundering and Combating the Financing of Terrorism, Risk Management policy is defined and “Obliged parties shall develop a risk management policy within the scope of the compliance policy, by paying attention to the scale of their business, business volumes and the nature of the transactions they conduct” is indicated. The purpose of risk management policy to enable the definition, grading, monitoring, assessment and mitigation of financial, reputational and operational risks which our Bank or employees could expose due to such reasons as benefiting of the services presented by our Bank with the purpose of laundering proceeds of crime and financing terrorism or non-compliance with the Law and regulation and communiques issued as per the Law and to define the measures within Bank which will be implemented for the principals of customer due diligence at minimum level.
Risk management activities cover the below given points at minimum level:

- To develop risk defining, grading, classifying and assessing methods on the basis of customer risk, service risk and country risk,
- Grading and classifying services, transactions and customers as per the risks,
- To enable the monitoring and controlling of risky customers, transactions or services; reporting them in a way to warn the related departments, developing the required operation and control rules to perform the transaction with the approval of its high authority and to enable the auditing when it is deemed necessary,
- Retrospective assessment of coherence and efficiency of risk defining and assessment methods, risk grading and classifying methods through case samples or performed transactions; reassessment and updating as per the results concluded and developing conditions,
- Following up the national legislation and recommendation, principle, standard and guidelines on the issues falling into the scope of risk introduced by the international institutions and conducting the required improving studies,
- Periodic reporting of risk monitoring and assessment results to the Board of Directors.

The client's risk profile assessment is carried out at the beginning of the business relationship, taking into account the customer, country and service risk factors identified in this policy. However, the comprehensive risk profile of some customers may change or be more clear when the transactions begin. This requires continuous monitoring of customer transactions and updating of the customer risk classification when necessary. Within this scope, the required information infrastructure and control points are established for the risk-based and continuous monitoring of transactions for both continuous business relationship and non-continuous business transactions, i.e. transactions of walk-in customers.. The awareness of the Bank personnel who contact with the customer and/or in the process of carrying out the said transactions is also increased and kept up to date by arranging regular training activities and informing them about current developments.

When a customer is risk-graded, information such as job/vocational knowledge, nationality, country of residence, activity area/sector, account opening purpose, transactions performed, and many other factors are assessed, and monetary or any other thresholds (number of transactions, frequency etc.) can be created. Acceptable risk rate is determined by making a scoring according to the thresholds created and the assessed factors. Customers and transactions that are below the acceptable risk rate are reviewed less intensively. These customers are evaluated for Alternatif Bank as a normal customer. The determination of acceptable risk limits is made by the Legislation and Compliance Department, taking into account the subjective and objective evaluation requirements of the Bank.

If there is an actual risk in the customer profile regarding the laundering proceeds of crime and financing terrorism, the transaction/customer is considered in high risk category, regardless of whether there is any threshold and exception in such cases.

A healthy monitoring and control process requires that information, documents and records of the customer are up-to-date under the continuous business relationship. Even under the condition that a new transaction is not carried out by the customer, and a new information available about the customer, the bank records and documents belonging to the customer are updated and confirmed. In addition, the correctness of the telephone and fax numbers and e-mail addresses of customers is confirmed by contacting them using these means in the framework of a risk-based approach.

1.1. CUSTOMER RISK

Our Bank may be exposed to risks, if the field of activity in which the customer operates, allows intensive use of cash, merchandise of valuables, or frequent international transfer of funds, if the customer or those who act on behalf of the customer or on their account, should act to launder crime proceed or to finance terrorism. Below principles are applied in order to prevent this.

1.1.1. Principles on Customer Due Diligence

Establishing the identification, which is the most important part of identifying the customer, is done according to the rules indicated in the Regulation on Measures Regarding Prevention of Laundering Proceeds of Crime and Financing of Terrorism, which is published in the Official Gazette dated 09/01/2008 with the number 26751.

During the approval process of the Customer, besides verifying the identification and address, the consistency of submitted documents and information, the customer's reason for choosing the bank and opening an account, the customer's occupation and his/her main income generating field of business, the work address and if possible information about their buyers and sellers must be obtained.

During the establishment of permanent business relationship, in addition to the information and documents which must be received for verification of identity, the documents indicated on Account Opening Instruction should be received as well.

Customer identification must be completed;

- Regardless of the amount while establishing permanent business relationship,
- When the amount of a single transaction or the total amount of multiple linked transactions is equal to or more than 20.000.-TL
- Regardless of the amount in cases requiring STR;
- When the amount of a single transaction or the total amount of multiple linked transactions is equal to or more than 2.000.-TL in wire transfers;
- Regardless of the amount in cases where there is suspicion about the adequacy and the accuracy of previously acquired identification information

For the determination of the real beneficiary, in Banking Service Agreements arranged with customers during the account opening, a statement is taken for the accounts opened and to be opened in Alternatif Bank and the transactions made over these accounts are made on the customer's own name and account; and in case the customer enters a transaction on behalf of someone else's name or account on these bank accounts, the person will inform the bank immediately within the scope of the Law No. 5549 and related sub-legislation.

Announcements are made in branches and locations, wherever customers served, to remind customers their responsibility for declaring the identity of persons if they enter any transaction or open an account on behalf of someone else's name and account.

A reasonable investigation should be made to reveal the actual beneficiary if the person is suspected of acting on his/her behalf but on behalf of another person even though the person does not declare that he/she does not act.

When the customer declares that he/she acting on behalf of someone else's, the identity and authority status of the person who requests the transaction and the identity of the person who is acted on his/her account are determined within the principles specified in the Identification Instruction and Account Opening Instruction of our the Bank.

In the establishment of permanent business relations with legal entities registered with the Trade Registry, the identity of the real person partners who have a share of more than 25% in the legal entity shall be determined as specified in the Account Opening Instruction. In cases where there is a suspicion that the natural person holding 25% or of the legal person's shares is not the beneficial owner or where there is no natural person holding a share at this rate, necessary measures shall be taken in order to detect the natural person(s) who is/are ultimately controlling the legal person. And natural persons detected shall be considered as beneficial owner.

In cases where the actual beneficiary can not be identified in the above scope, the real person or persons with the highest executive authority registered in the commercial register shall be considered as the actual beneficiary of the company. The identification of the real person beneficiary is carried out with one of the identification documents specified in the Account Opening Instruction of the Bank. Within the scope of

permanent business relationship, the identity of the legal entity partners of the company who holds 25% or more shares in the entity's capital is also determined in accordance with the principles specified in the Account Opening Instruction.

Within the scope of permanent business relationship with other legal persons and uncorporated organizations, necessary measures shall be taken in order to detect the natural persons who is/are ultimately controlling the legal person. In case where the beneficial owner is not detected, the natural persons holding the position of senior management shall be considered as beneficial owners. The identification of those real beneficiaries are carried out with one of the identification documents specified in the Account Opening Instruction.

If transactions are performed by another person on behalf of the real customer, identification of the person acting on behalf of the customer is done through the identification documents. In addition, the authority status of anyone moving on behalf of the client is confirmed by a notarized proxy. If the identity of the customer who is acted on behalf of the customer can not be determined through the identification documents, it shall be done through a notarized proxy. In case the identity of the customer has been determined due to previous transactions, the requested transactions can be done by someone else acting on behalf of the customer with the written instruction of the customer.

In transactions requested by the legal representatives acting on behalf of minors and persons under legal custody, the authority of those appointed as guardian by court decision, curators and trustees are verified through the original or notarized copy of the relevant court decision. In the case of parents requesting transaction on behalf of children, it is sufficient to identify the child for whom the transaction is requested and the identity of the parents requesting the transaction.

After documents which are subject to verification are submitted, legible photocopy or electronic image of their originals or notarized copies shall be received in order to submit upon request of authorities.

Obliged parties shall verify the authenticity of documents as much as possible by applying to person or institution arranging the document or to other competent authorities in cases where they suspect of the authenticity of documents used for the verification of the information recorded. In this context, in the ongoing business relationship established with legal persons registered in the trade registry, the authenticity of the documents presented are confirmed using the online database of Union of Chambers and Trade Registrars. Information obtained in transactions with real persons is verified by using the "Identity and Address Sharing System Database" which provided by the Ministry of Interior, General Directorate of Population and Citizenship Affairs. The correctness of the information regarding the telephone and fax number and the e-mail addresses of the customers is confirmed by contacting them in the framework of the risk-based approach using these means.

In accordance with the provisions of the Regulation on Measures and the Related Communiques issued by FCIB,

a) In transactions carried out between financial institutions and our Bank

b) In transactions where the customer is a public administration or quasi public professional organization in the scope of Public Financial Management and Control Law No. 5018,
c) In establishing a business relationship within the scope of salary payment by accepting a batch of customers,
d) In transactions related to pension schemes that provide retirement benefits to employees by way of deduction from their salaries and of pension agreements,
e) In transactions where the customer is a public company and its shares are listed on the stock exchange.

simplified measures can be applied in terms of measures for the identity recognition of the customer. Details concerning this issue are set out in the sub-directives issued in the context of this policy. In cases where the risk of money laundering or financing terrorism may arise, simplified measures are not applied to the identity recognition of the client.

The business relationship may be established or dealt with by reliance on the measures taken by third parties. Identification of the customer, the persons acting on behalf of the customer, and the real beneficiary and the information obtained about the purpose of business relationship or the purpose of the transaction can be obtained by another financial institution by reliance on the measures taken by this institution. In this case, the ultimate responsibility within the scope of the regulations related to the Law belongs to our Bank, which rely on the third party.

Reliance on third parties shall be possible only if it is ensured that;

a) The third parties have taken enough measures which will meet the requirements of customer identification, record keeping and the principles of “customer due diligence”, and are also subject to regulations and supervision in combating money laundering and terrorist financing in accordance with international standards if the third parties are resident abroad,
b) The certified copies of documents relating to customer identification shall immediately be provided from the third party when requested,

In this context similar to establishing business relationship with correspondent banks, to specify the third parties to be relied, a careful due-diligence is carried out. Within this due-diligence, information is provided on the reputation, and reliability of the bank, adequacy of the internal and external audit on the bank, whether it is punished or not related to money laundering and financing of terrorism. The institution to be relied as third party shall also be asked to fill in the Correspondent Account Survey Form.

Legislation and Compliance Department checks whether the financial institution to be relied as a third party is investigated and charged for money laundering or terrorism financing. The Department determines whether the financial institution will be trusted as a third party or not by evaluating the practices and controls of the institution related to prevention money laundering and financing of terrorism, know your customers practices and monitoring and control systems.

When a business relationship established or transaction is made by relying on a third party, the identity information of the customer is immediately received from the third party.

The reliance on third-party principle does not apply if the third party is located in high risk countries in terms of money laundering and financing of terrorism.

In cases where customer identification can't be done or the information on the purpose of the business relationship can't be obtained, the business relationship is not established and the requested transaction is not performed. In this context, an anonymous account or account in a fictitious name can not be opened.

In subsequent transactions of the customer, whose identity is determined by the bank within the scope of continuous business relationship, the updateness of information is checked. In this context, the identity document of the customer, and if the transaction is executed on behalf of another person, a certificate of authority is obtained and the information on these documents is compared with the information in the Bank system. If there is no change in the information previously received, there is no need to have photocopies or electronic samples of the documents submitted. After the comparison, the name and surname of the real person who has the related affirmative action are written and a signature sample is taken. In the event that the information provided on the previous documents differs from the information on the valid identity and authority documents provided, the identification of the person is redetermined and the information held in the Bank systems is updated by verifying it from the relevant databases. In subsequent transactions performed via non-face-to-face systems, necessary measures are taken to verify the identity of the customer and to ensure that the information contained in Bank's systems are up-to-date.

If the customer identification and its verification which are required to be conducted due to suspicion on the adequacy and accuracy of the previously obtained customer identification information cannot be carried out, the business relationship shall be terminated.

In such cases, whether or not there is a suspicious transaction, will be evaluated separately.

The resolutions taken in line with the Law No. 6415 on the Prevention of the Financing of Terrorism and resolutions published in Official Gazette on asset freeze and abolishment of such resolution to asset freeze is implemented without any delay.

Required measurements are taken not to establish business relationship with the blacklisted persons and institutions as per the international financial system as well as other similar international lists (USA, European Union etc.) to which our banks have to comply.

If the Compliance Department assesses that working with a customer in the high risk group would be unfavourable for our Bank, the business relationship could be terminated with the approval of the Executive Vice President of Marketing, who is in charge of the customer in question. In

the event that there is a disagreement between the Legislation and Compliance Department and related VP about the termination of the business relationship with the high-risk client, the issue is presented to the Management Risk Committee for evaluation.

1.1.2. Customer Acceptance Criteria

1.1.2.1. Persons and entities that will not be accepted as a customer

a) Persons Whose Real Identities and Addresses Cannot be Determined. Persons and entities who want to open an account under a different name, are refraining from filling the customer introductory information and forms, are being reluctant in this matter or are giving deceptive information that cannot be confirmed,

b) Persons and entities that are blacklisted by official institutions publishing lists on laundering of crime proceeds and terrorism financing.

c) Shell Banks: Shell Banks and financial institutions that do not have a physical address in any country, do not have at least one employee who works full time, that are not subject to audit or permission of an official authority regarding banking operations and records, that are not an establishment of a recognized bank subject to acceptable regulations and audit procedures related to prevention of laundering crime income and banking operations, should not be accepted as a customer and no transactions what so ever should be done on behalf of these types of persons or institutions.

d) Account opening and performing brokerage for their collection and payments to the name of gambling and betting companies without having the authority to arrange or conduct chance games with fixed odds betting or pari-mutuel betting as per The Law No.7258 on Football and Other Sports Competitions Betting and Gaming Regulation or to the name of such companies which run betting activities against the procedures and principles set out in the legislations is not allowed.

e) System operators, payment institutions and electronic money institutions which do not have the official activity authorization obtained as per the Law No.6493 on Payment and Securities Settlement Systems, Payment Services and Electronic Money Institutions.

f)Financial institutions (brokerage house, bank, leasing, factoring, consumer financing, portfolio management, investment consultancy companies, investment funds etc.) without having activity authorization obtained from CMB and/or BRSA which want to operate business in Turkey or Turkey representation offices of such institutions resident abroad;

g) Companies and institutions which conduct the brokerage activities for the payments of persons and institutions under embargo and not having real commercial activity.

1.1.2.2. Real and legal entities that need additional close attention to be accepted as a customer

a) Correspondence relationship is established as per the principles and procedures indicated in Establishment and Follow-up the Correspondence Relationship Procedure. Transactions are performed in line with the correspondence relationship types and country risk situation as indicated in the mentioned procedure.

Apart from the relationship type and country risk, in the establishment of correspondence relationship, our International Financial Institutions will make an inquiry on whether or not the banks which could be accepted as Correspondent has been subject to investigation of laundering proceeds of crime or terrorism financing and imposed any penalty and obtain reliable information or from related databases about their field of business, reputation and the sufficiency of the auditing by making use of the information open to the general public and based on this information, such documents as Banking License, Articles of Association/Registry Certificate of the Bank, Correspondent Questionnaire Form and Patriot Act Certificate will be received and communicated with Legislation and Compliance Department.
In its examination, Legislation and Compliance Department checks whether the correspondent bank with whom the relationship will be established has been subject to any investigation or penalty due to money laundering or terrorism financing. It also submits its opinion by assessing the bank's implementation and controls for money laundering and terrorism financing, regulations on "know your customer" principle and customer identification as well as its monitoring and control systems.

Within the context of establishing a correspondent relationship, the responsibilities of Alternatif Bank and its counterparty financial institution, are clearly defined by a contract signed by these institutions. Instead of signing a contract, mutually applied AML / CFT questionnairies can also be used for this purpose.

No relationship will be established with banks allowing their accounts to be used by Shell Banks.

b) Politically Exposed Persons; Such persons as politicians holding high level civil service, soldier, police, prosecutor, bureaucrat, high level public institution executives/ municipality managers fall into the scope of the definition of politically exposed persons. In the case of account opening request by the mentioned persons holding high level civil service, following to the account opening, Legislation and Compliance Department should be informed.

c) Foundations and Associations (Charitable Foundations and Aid Organizations): In the case of an accounting opening for the non-profit aid organizations, approval should be taken within the scope of related procedures by implementing comprehensive "know your customer" principles due to the fact that mentioned institutions are open to abuse and can be misused by the terrorist organizations by creating the image of legal assets and using the funds saved here to the benefit of theirselves.

d) Account opening for non-residents and to the ones having foreign nationality (legal and real) or legal entities whose shareholders are foreigners is subject to approval and the account should not be opened without obtaining the required approval within the scope of related procedures

e) Companies with Bearer Shares : Accounts which will be opened for companies that have issued bearer shares are considered as high risk group accounts. Especially companies founded in offshore regions issue bearer shares. It is possible to detect such cases from the companies' main contracts. Therefore, careful examination of the main contracts of both resident and non-resident companies is of vital importance. Prior to opening accounts for such companies, verification of the obtained information on company owners, real beneficiaries and financial status should be sought from relevant sources.

f) Residents in off-shore regions

g) Payment and Electronic Money Institutions,

h) Companies acting as intermediaries in the purchase and sale of Bitcoin and similar crypto currencies

i) Account opening via power of attorney is subject to approval and the account should not be opened without obtaining the required approval within the scope of related procedures.

j) Customers Active in Business Sectors Sensitive to Laundering of Crime Proceeds,

It is recommended that extreme due diligence is exercised while opening an account for real and legal entities active in the below given industries and profession groups and transactions related to these must be closely monitored.

- Exchange Offices,
- Jewelers, traders of precious stones and metals (such as gold and diamonds),
- Travel agencies, passenger and cargo carriers,
- Operators of casinos and halls for gambling,
- Dealers of luxury vehicles,
- Dealers of antiques, art galleries, carpet traders,
- Major real estate brokers (including their agnecies and representative offices)
- Those leasing air and sea crafts

- Financial Institutions seeking to open a payable through account
- Those operating in cash based business (parking lot operators, gas stations, restaurants, lottery parlors, newspaper kiosks and distributors, etc.).

1.2. COUNTRY RISK (CUSTOMERS RESIDENT IN OR CONNECTED WITH HIGH RISK GEOGRAPHICAL PLACES AND THEIR PROCEEDINGS)

High risk countries are identified as given below:

- Countries which have been subject to sanction at international scale within the framework of resolutions of United Nations Security Council due to their policies and implementations related to laundering proceeds of crime or terrorism financing,
- Countries listed in FATF's Non-Cooperative Countries and Territories list
- Countries identified as bearing high risk of laundering proceeds of crime and terrorism financing and which have been subject to sanction by the European Union or United States of America
- Countries announced by the Ministry of Finance as not having sufficient regulations regarding prevention of money laundering and financing of terrorism and as non-cooperative in the fight against these crimes.
- Tax heavens, off-shore districts, off-shore finance centers declared by OECD, IMF and such similar institutions,
- Countries which do not have regulations in an adequate level about prevention of laundering proceeds of crime and terrorism financing, in which legal order is not performed, where fraud, smuggling, corruption is prevalent and criminality rate is high as well as countries whose financial transparency and standards, public transparency and accountability indicators are bearing risk

Country risks are monitored by categorizing and grading them as low, middle, high and red level risks.

1.3. SERVICE RISK (BANKING PRODUCTS BEARING RISK)

a) Cash Transactions.

b) In fund transfers which have been sent, the address details of the sender and the name and address details of the beneficiary are detected by clarifying the identification of the sender, whether the transfer will be done to his/her name or any other person. Also, the amount to be transferred should also be checked and it must be consistent with the business of both sender and beneficiary. The information stated in Article 24 of Regulation on Measures Regarding Prevention of Laundering Proceeds of Crime and Financing of Terrorism should be indicated in the transfer message. In the case of receiving electronic transfer message which do not cover the

information stated in the mentioned article, financial institution performing the fund transfer is requested to complete the missing information. If the information is not completed the fund is returned. Correspondence relationship with the institution sending its messages with missing information in spite of the warning is terminated.

In received transfer messages, a detailed examination in the scope of suspicious transactions is conducted by paying the required attention to the received ones in which the information on the issuer and beneficiary is missing.

c) Accepting Personal Cheques Drawn on Foreign Banks for Collection:

d) Internet and ATM Transactions.

e) International payments performed to companies whose field of business cannot be defined.

f) Payments below level conducted to avoid identification and information controls are examined by means of sampling whether these transactions are performed due to avoid legal obligations or not after they are detected and analyzed with the help of software.

g)Safe-deposit box transactions are monitored via customer profile, visit frequency and such similar criteria.

By taking into consideration customer risk, service risk and country risk criteria explained above and by defining the threshold values regarding the number and amount of the transactions materialized by the the customer, risky customers are determined, and transactions of these customers will constantly be monitored through reporting.

2. MONITORING AND CONTROL ACTIVITIES

The Bank conducts the monitoring and controlling activities by paying attention to the nature of the transactions performed by its customers.

The purpose of monitoring and controlling is to protect the Bank against the risk and continuously monitor and control whether or not the Bank activities are being conducted in line with the Law, regulation and communiques, internal policy and procedures.

In this scope, monitor and control activities conducted in the Bank within the scope of prevention of laundering proceeds of crime and terrorism financing are given below:

- Customers and transactions in high risk groups are monitored and checked.
- Transactions conducted with risky countries are monitored and checked.
- Customer surveillance lists are created.
- During the term of business relationship, continuous monitoring of the fact that whether the transactions conducted by the customer are consistent with information of the customer's job, risk profile and fund resources is ensured.
- Complex and unusual transactions are monitored and checked.
- Transactions exceeding the amounts determined separately for real and legal entities within a certain period are monitored and checked.
- Amounts that need identity verification when considered as a whole are monitored and checked.
- Control and completing the missing parts of the documents and information on the customer which are required to be kept as a soft copy or hard copy and updating thereof are ensured.
- The information in the Electronic Fund Transfer messages is checked, if found missing, it is completed and updated.
- Control of the transactions which have been performed by using the systems to perform transactions not face-to-face such as internet and ATM is done.
- Cash activities over the pre- determined treshold values are monitored and checked.
- News related to Money Laundering and Terrorism Financing which is reflected to the media is followed up within the scope of Media Follow-Up Instructions and they are examined whether they pose a risk against our Bank or not. When some negative news about our customers or persons making transaction with our Bank, it is ensured to perform the suspicious transaction reporting, stop the transactions in necessary cases or terminate the business relationship with the customer.

3. SUSPICIOUS TRANSACTION REPORTING and SUSPICIOUS TRANSACTION NOTIFICATION REQUESTING DEFERRAL

A suspicious transaction is an event where there is information, suspicion or any matter that may evoke the suspicion that a possession which is part of a transaction made within or over our bank or which is part of an attempted-transaction, is gained by illegal means or used for illegal aims, terrorist attacks or that the possession is used by terrorist organizations, terrorists or people who finance terror.

The definition of suspicious or unusual transaction covers "use of the asset subject to transaction for illegal purposes" in addition to acquirement of it through illegal ways, which demonstrates that it aims essentially to prevent financing of terrorism. In this scope, cases where there is any information, suspicion or reasonable grounds to suspect that the funds are used for terrorist activities or by terrorist organizations, terrorists or those who finance terrorism, or that the funds are related or linked to terrorist organizations, terrorists or those who finance terrorism shall be subject to suspicious transaction reporting.

Suspicious transactions are notified to the Compliance Officer by the related branches or Head Office departments. In addition, transactions found suspicious during routine audits by the Internal Audit and Internal Control Departments are advised to the Compliance Officer. The Suspicious Transaction Reports, that are sent to AML Unit, is evaluated considering the relevant laws, regulations and communiqués by the

Compliance Officer. Then, Compliance Officer decides whether to send the report to Financial Crimes Investigation Board or not. In cases where it is not deemed necessary to send the report to FCIB, the form together with the written statement about the reason for not sending the report, are kept by the Compliance Officer to present to authorities when necessary.

The Suspicious transactions, determined by the Compliance Department during the monitoring and control activities, are sent to the Financial Crimes Investigation Board (FCIB) by the Compliance Officer after the necessary investigation has been conducted.

With regards to suspicious transactions reporting with a deferral call, if there is suspicion that a transaction attempted to be conducted at the counters of or through the Bank or a transaction that is currently in the works, is linked with money laundering or financing of terrorism crime, then without the need for a court order, the transaction may not be realized until the Bank is notified with the decision of the Ministry of Finance by the Presidency of the FCIB; and in line with the notified decision the transaction will either be realized or not. In case the decision on the transaction is not relayed to the Bank by the Presidency of FCIB within 7 business days, then the transaction subject to the deferral call will be materialized by the Bank. The concerned 7 business days period commences on the following day of the actual suspicious transaction reporting. Our branches and/or departments cannot abstain from submitting any kind of information or document on time which is requested by the Compliance Officer for the sake of transactions reported or to be reported.

It is compulsory to report Suspicious Transactions in 10 working days time after (in situations where there is a risk of delay, immediately), Suspicious transactions that require transaction deferment are instantaneous to FCIB as soon as the suspicion occurred.

Those who report suspicious or unusual transactions and other bank personnel, who are informed of the transaction, shall not reveal the reporting to anyone other than auditors who are in charge of audit of obligations and courts in course of a trial. Internal reports are also confidential. Attention and care at the utmost level which is required as per the legislation is paid to the issues related to the confidentiality and security of the suspicious transaction reporting and internal reporting performed in the Bank within this scope as well as the protection of the parties of such reporting. Information is not given to those customers whose transactions have been suspended / unperformed and that has gone through a Suspicious Transaction Notification Requesting Deferral, and the notification of their rights is made within the scope of the explanation.

4. COMPLIANCE OFFICER

4.1. Appointment

The Compliance Officer refers to a senior employee directly reporting to the Board of Directors or member/members assigned by the Board of Directors. The person who will be appointed as the Compliance Officer must have the specific attributes indicated in article 17 of the Regulation On Program of Compliance with Obligations of Anti-Money Laundering and Combating the Financing of Terrorism

Besides sales, marketing and internal audit, other duties which will not hinder conducting of compliance program can also be under the responsibility of the Compliance Officer.

Once the Compliance Officer is appointed, this will be notified to the FCIB together with the documents indicated in Article 16 of the Regulation On Program of Compliance with Obligations of Anti-Money Laundering and Combating the Financing of Terrorism–If no negative remarks are given within 30 days after the date of notification to the FCIB, the appointment of the Compliance Officer will be finalized.

4.2. Duties and Responsibilities of the Compliance Officer

1. Making the necessary arrangements to ensure compliance to the Law and Regulations and to ensure the necessary communication and coordination with FCIB,

2. Creating policies and procedures regarding prevention of laundering crime proceeds and terrorism finance and submitting them to the approval of the Board of Directors,

3. Creating risk management policies, conducting risk management activities,

4. Creating surveillance and control policies and conducting activities related to this,

5.Getting the approval of the Board of Directors for training programs on prevention of money laundering and financing terrorism and making sure the approved training programs are carried out effectively,

6. Evaluating suspicious transactions and notifying FCIB after thorough investigation.

7. Taking necessary measures to ensure confidentiality of notifications and other related matters,

8. Keeping information and statistics regarding internal audit and training activities in an orderly manner and sending them to FCIB within the legal deadlines,

9. Giving the information and documentation requested by FCIB according to the format and the method indicated by FCIB.

10. Quarterly reporting to Board Audit and Compliance Committee about the activities of the Compliance Department.

11.Within the framework of compliance to the legislation on Prevention of Laundering Proceeds of Crime and Terrorism Financing, Compliance Officer is authorized to request any kind of document and information related to his/her own area of duty from all groups, departments and branches within the entity of the Bank and to reach such mentioned information/documents on time.

12.Compliance Officer acts in a well-intentioned, reasonable and honest with an objective and independent will while conducting his/her duties. Board of Directors ensures to provide adequate number of staff and resource allocation to the Compliance Department reporting directly to the Compliance Officer and responsible from conducting the compliance program with the purpose of enabling the Compliance Officer perform his/her duties and responsibilities as per the legislation on Prevention of Laundering Proceeds of Crime and Terrorism Financing in an efficient way, by considering such issues as the size, transaction volume, branch and personnel number of the Bank or the level of risks which could be exposed to.

4.3. Resignation of Compliance Officer

In case the compliance officer leaves his post temporarily for vacation or illness, the person who will be his deputy must have the conditions in Article 17 (except paragraph d) of the Regulation On Program of Compliance with Obligations of Anti-Money Laundering and Combating the Financing of Terrorism-The identification of the deputy and contact information will immediately be given to FCIB. Proxy period cannot exceed 60 days within one calendar year. Deputy has all the duties, powers and responsibilities of the Compliance Officer. Compliance Officer cannot be held responsible for the duties exercised by his deputy

In the event of the Compliance Officer leaving his job permanently, the new Officer will be appointed within maximum 30 days and FCIB will be notified. Until a compliance officer is appointed, the above explained proxy rules will be applied. .

5. INTERNAL AUDIT

Efficiency and sufficiency of the entire compliance program constituted by the Bank is audited by the Bank's Internal Audit Departments with the purpose of providing assurance to the Board of Directors.

Audit for the purpose of AML-KYC is performed by the Internal Audit Department in the Bank. Audits are performed on a yearly basis with a risk based approach covering the subjects of risk management of policies and procedures, whether monitoring and control and training activities are sufficient or not, sufficiency and effectiveness of the Bank's risk policies, if the transactions are being conducted in compliance with the Law and Regulations and Manifestos formed according to the Law and to the policies and procedures of the Bank.

The deficiencies determined during surveillance and controls, along with risky customers, services and transactions will be included in the audit.

While the inspections by the Board of Inspectors, can be exercised within the regular yearly program together with branch audits, if deemed necessary, they can be exercised exclusively as well.

Deficiencies, mistakes and misconducts detected at the end of the audit as well as opinions and suggestions to prevent them from occuring again will be reported to the Board of Directors or to the representative member/members of the Board of Directors.

Within the scope of internal audit activities, statistical information containing annual transaction volume of the Bank, total number of personnel and number of branches, number of audited branches, dates of audits, total audit period, information on the personnel working in the audit and the number of audited transactions will be reported to FCIB by the Compliance Officer until the end of March every year.

6. TRAINING POLICY

The purpose of the training policy is to enable the compliance to the obligations imposed by the Law and regulations and communiques published on the basis of the Law, to constitute a corporate culture by increasing the responsibility awareness of the personnel about corporate policy and procedures and issues with a risk-based approach and to ensure the information updating of the personnel.

Training text regarding Prevention of Laundering Proceeds of Crime and Financing of Terrorism is prepared by the Compliance Officer. This text will be prepared to at least cover the subjects of;

- Concept of laundering crime proceeds and financing terrorism,
- Stages and methods of laundering and examples of case studies,
- Regulations regarding prevention of laundering crime proceeds and financing terrorism,
- Risk areas
- Company Policy and Procedures,
- Rules on identifying the customer, rules related to notification of suspicious transaction, conservation and presentation obligations within the regulations related to the law,
- Obligation to give information and documentation, applied sanctions in case the obligations are not followed and international regulations on money laundering and financing terrorism

Regarding the training activities within the year;

Information and statistics related to training dates, area or cities the training will be given, training method, total training hours, number of personnel to be trained and its ratio against the total number of personnel, breakdown of personnel to be trained according to their departments

and titles, contents of the training, titles and expertise areas of the trainers will be advised to FCIB until the end of the month of March of the following year.

Training is given to at least cover all the employees working in the marketing and operation departments including the branch managers in the branches, and the employees in the Operation, Marketing, International Financial Institutions, Fund Management, Credit Allocation, Restructing, Monitoring, Litigation, Financial Control, Accounting, Law, and Internal Systems departments in the Head Office.

Training is given each year according to the jointly determined program of the Compliance Officer and Training and Development Department

Training is given via the intranet for the existing and newly recruited personnel. In group recruitments (Management Trainees) face to face training can be given by either the Compliance Officer or an expert trainer.

If necessary, face-to-face meetings can also be organized by gathering the personnel in one place by the Compliance Officer and the Training and Development Department's joint decision.

Training given through the Intranet is repeated at least once in two years' period the personnel are tested on the subjects at the end of the training. Besides all of the personnel are subject to measurement and evaluation through an electronically processed exam concerning the training contents every year. Policies and training methods may be reevaluated depending on the test results.

7. OBLIGATION OF DOCUMENT AND INFORMATION SUBMISSION- RETAINING OF THE RECORDS

In Our Bank, the reporting activities in the scope of continuous information submission and requests received from FCIB and institutions and officers authorized to request information and document, for any kind of information, document and records related to them in any environment, for accessing such records or submission of all information and passwords in a correct way and without any missing detail to make them readable are performed with attention and care at the utmost level.

As per the effective Law and provisions of the Regulation and Communique issued for its implementation, the Bank ensures the retaining of documents in any environment related to obligations and transactions which are imposed by the mentioned Law for eight years since the date on which such documents were drawn up, the books and records since their last registration date, documents on customer identification since the date of last transaction and the Bank submits these documents to the authorized persons when it is required.

Suspicious transaction reporting and the attachments thereof are under the scope of retain and submission obligatory.

8. CORPORATE PROCEDURES

Detailed issues such as the persons who are responsible from the all measures and operating rules defined in the scope of is Compliance Policy, who or which departments will be responsible from the approval, performing, reporting and monitoring of the transactions as per the specific risk limits will be defined with the sub-regulations which are issued or to be issued with the names of procedure, instruction, form and list.

Procedures, instructions, forms and lists which will be issued within the framework of this policy are formed in a written way which is aligned with the Law and regulation and communiques issued as per the Law under the supervision and coordination of the Compliance Officer by obtaining opinion of the our departments. Compliance Officer is authorized for the mentioned sub-regulations and changes to be made in sub-regulations and further approval from the Board of Directors is not required.

9. AUTHORITY and RESPONSIBILITY

Conducting the compliance policy effectively is under the ultimate responsibility of the Board of Directors.

The Board of Directors is authorized and responsible from appointing the Compliance Officer, determining clearly and in writing the authority and responsibility of the Compliance Officer and the compliance unit, approving corporate policies, training programs and necessary amendments according to new developments, evaluating the results of risk management, conducting surveillance and controls within the scope of the compliance program, taking the necessary measures to eliminate the detected mistakes and deficiencies and ensuring all the activities within the scope of the compliance program are performed effectively and in coordination. The Board of Directors can assign part or all of its powers within this scope to one or more members of the Board.

This Compliance Policy enters into effect with the approval of the Board of Directors. In the case of partial or fully delegation of authorities in this respect by the Board of Directors to one or more than one board member in a written way, revisions to be made in the Compliance Policy enter into force with the written approval of that member or members and if such an authority delegation is not applicable the revisions become valid with the approval of the Board of Directors.

Revisions to be made in the Compliance Policy will be communicated to the Head of FCIB within thirty days at the latest since the date of revision.