KOC FINANSMAN A.Ş.

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

June 2021

INDEX

1. INTRODUCTION

As known, this subject is regulated by Financial Action Task Force – FATF, established with the purpose of prevention of money laundering and financing of terrorism in the international arena and requirement for member countries to comply with the regulations and principles set out by FATF has been turned into an obligation. Our country is also a member of FATF and, in this context, compliance with international legal arrangements, preparation of regulations and performance of regulatory activities is entrusted to the Financial Crimes Investigation Board (MASAK), established as a board attached to the Ministry of Treasury and Finance.

Koç Finansman A.Ş. (Company) is a pioneer company of finance sector in Turkey. Yapı ve Kredi Bakası A.Ş. displays sensitivity at highest level for full compliance with provisions of 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, taking into consideration at the same time financial repercussions of the matter and its effects on the community.

2. DEFINITIONS

Proceeds of Crime : Proceeds of crime means assets originating from criminal activity.

Money Laundering Offence : Money laundering offence means the offence defined in article 282 of the Turkish Criminal Code No. 5237 dated 26/09/2004.

Article 282 of the Turkish Criminal Code No.5237:

- Any person who takes away the assets acquired as a result of an offense which requires minimum six months or more punishment of imprisonment, or carries the same to a foreign country to be subject to various transactions in order to hide illegal source of these assets and to give the impression that they are acquired in the lawful manner, is punished with imprisonment from three years to seven years, and also imposed punitive fine up to twenty thousand days.

- A person who, without participating in the commitment of the offence mentioned in first paragraph, purchases, acquires, possesses or uses the proceeds which is the subject of that offence knowing the nature of the proceeds shall be sentenced to imprisonment from two years up to five years.

- Where this offence is committed by a public officer or professional person in the course of his duty then the penalty to be imposed shall be iincreased one half.

- Where this offence is conducted in the course of the activities of an organization established for the purpose of committing an offence, the penalty to be imposed shall be doubled.

- Where a legal entity is involved in the commission of this offence it shall be subject to security measures.

- In relation to the offences defined in this article, no penalty shall be imposed upon a person who directly enables the securing of financial assets, or who facilitates the securing of such assets, by informing the relevant authorities of the location of such before the commencement of a prosecution.

Financial Crimes Investigation Board (MASAK): It is commissioned and authorized to combat laundering of proceeds of crime. It is directly attached to the Ministry of Treasury and Finance.

Suspicious Transactions: Suspicious transaction means presence of any findings, suspicions or grounds for suspicion in undertaken or attempted transactions with or through designated persons that the assets involved in the transaction were acquired illicitly or used for illicit purposes or were used for terrorist activities or terrrorist organizations or by terrorists or by persons financing terrorist activities or were associated with or related to the foregoing.

Designated Parties : Designated parties mean those institutions designated as responsible for discharging the obligations (such as identification, suspicious transaction reporting etc.) set out as preventive measures to be taken for combating laundering proceeds of crime

Compliance Officer: It is the officer who is employed and given the necessary authority to ensure compliance with obligations set out in the Law and regulations that come into force in accordance with the Law.

Deputy Compliance Officer : The officer who is employed with the necessary authority to ensure compliance with obligations and assigned by written from some or all of Compliance Officer's authority and responsibilities enforced by the legislation.

Continuing Business Relationship: It is the business relationship of a continuing nature between the Designated Parties and the customers established for providing services such as account opening, sanctioning credit facilities, issuing credit cards, allocating safe deposit boxes, financing, factoring, financial leasing services.

FATF : Financial Action Task Force is an international organization established to combat money laundering and financing of terrorism. Turkey is also a member of this organization.

Compliance Program : It is the entire body of measures referred to in article 5 of Regulation about Compliance Program Regarding Obligations Under Prevention of Laundering of Proceeds of Crime and Financing of terrorism.

Corporate Policies and Procedures : It refers to the regulations and instructions in which the details that have to be applied within the scope of the Corporate Policy on Prevention of Laundering of Proceeds of Crime and Prevention of Terrorism Financing are disclosed and announced to the Company.

Financial Institution: It refers to the obliged parties listed in subparagraphs (a) to (h) and (m) of the first paragraph of Article 4 of the Regulation on Measures to Prevent Money Laundering and Terrorist Financing and the Postal and Telegraph Organization Incorporated limited to banking activities.

Financial group: A group consisting of financial institutions resident in Turkey and their branches, agencies, representatives and commercial agents as well as similar affiliated units, which are affiliated with an institution whose headquarters is in Turkey or abroad or under control of such institution.

Main Financial Institution: It refers to the main institution responsible for the oversight of compliance at the financial group level with the obligations imposed by the Law and the regulations issued within the scope of the Law.

Enhanced Approval Mechanism: It refers to the approval of the compliance unit of financial institution or the higher echelon manager.

Politically Exposed Person (PEP): It refers to person who hold important public positions today or in the past, senior politicians, senior officials working in administrative and judicial bodies and/or in the armed forces or public economic enterprises, persons with significant powers in political parties, managers working in international organizations and organizations, and persons who hold positions equivalent to the positions listed in this definition, and all persons with whom all these persons have close ties to family members.

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

Asset : Asset means fund, proceeds, benefit and value derived from inter-conversion of them, owned or possessed or directly or indirectly controlled by a natural or legal person.

Freezing of Asset: Removal or restriction of the power of disposition over the asset for the purpose of preventing obliteration, consumption, conversion, transfer, assignation, conveyance and other dispositional actions of the asset.

Law no. 6415 on the Prevention of Financing of Terrorism : This Law herein, has been prepared within the scope of effective fight against terrorism and financing of terrorism for the purpose of determining the principles and procedures on implementing the "International Convention for the Suppression of Financing of Terrorism" dated 1999 and the United Nations Security Council Resolutions related to combating terrorism and the financing of terrorism within the context of this Law, on establishing financing of terrorism offence, and on freezing of asset with the aim of preventing financing of terrorism**.**

Law No. 7262 on Preventing the Proliferation of Financing Weapons of Mass Destruction: Law No. 7262 regulates rules and principles related to implementation of sanctions of the United Nations Security Council ("UNSC") regarding prevention of financing of proliferation of weapons of mass destruction.

3. PURPOSE AND SCOPE

In accordance with the regulations on Prevention of Money Laundering in Koç Finansman A.Ş., the Executive Board of Company is ultimately responsible for carrying out the whole compliance program adequately and efficiently appropriate for the scope and nature of activities of the obliged party.

Within this scope, the Board of Directors is authorized to and responsible for assigning Compliance Officer and Deputy Compliance Officer. The Board of Directors is authorized to and responsible explicitly determining in written form the authorities and responsibilities of the Compliance Officer and Compliance Department, ratifying institutional policies, annual training programs and amendments to be made in accordance with developments, assessing the results of risk management, monitoring, control and internal control activities carried out under the scope of the compliance program, taking required measures for timely elimination of the detected errors and deficiencies, and ensuring an efficient and coordinated performance of all the activities carried out under the scope of the compliance program.

The purpose of this corporate Policy is compliance with obligations relating to Prevention of Laundering of Proceeds of Crime and Financing of terrorism, determination of strategies to reduce contingent risk by evaluation of customers, transactions and services on a risk sensitive basis, determination of controls and measures, operational rules and responsibilities as well as raising the awareness of the employees of the Company on these matters in the Koç Finansman A.Ş.

Yapı ve Kredi Bankası A.Ş. has been assigned as Main Financial Institution in accordance with the decision taken by Board of Directors of Koç Holding. Companies within the Yapı ve Kredi Bankası Financial Group are allowed to share data within the group companies related to training, risk management, monitoring and control activities. In addition, data related with KYC, account and transactions in order to conduct internal audit activities (excluding suspicious transaction reports) can also be shared within the group companies.

All activities to be performed and measures to be taken within the Company in the frame of this policy are determined by related procedures, internal regulations and circulars issued by the Compliance Department of the Company. Preparation of mentioned procedures, their amendment consistent with circumstances and their implementation are within the powers and responsibility of Compliance Officer or Deputy Compliance Officer. All Employees are responsible for complying with this Policy and procedures and all applicable laws and regulations in the performance of their duties.

Failure to comply with or any breach of this Policy may give rise to disciplinary action against the relevant Employee in addition to the penalties contained in the local laws and regulations.

This Policy is notified to employees against their signatures or other methods declared by MASAK. The updates in the Policy will be published in related Financial Institution's Intranet and considered as notified.

4. RISK MANAGEMENT

The Company and/or Company employees employees face financial and/or reputational risk due to failure to fully comply with Law and regulations related to this Law or due to reasons such as benefiting from available services with the purpose of laundering proceeds of crime or financing of terrorism.

Taking into consideration the size of the Company, business volume and nature of transactions performed, a risk management policy should be in place as part of the Corporate Policy, covering definition of contingent risks, their grading, monitoring, evaluation and reduction.

Consistency and effectiveness of risk identification, classification and grading methods are evaluated by considering the past transactions and incidents. Concluded results are reevaluated and updated according to developing conditions. In addition to this, results of risk monitoring and evaluation are regularly reported to Audit Committee and Board of Directors.

Risk management consists of KYC principles, KYC rules, customer risk, service risk and country risk.

4.1. Know Your Customer Principles

KYC Principles include principles in order to comply with "Know Your Customer" rules, has an important place in FATF recommendations and also adopted by national and internation regulations in accordance with Prevention of Laundering Proceeds of Crime and Financing of Terrorism.

- ✓ Necessary controls are conducted and additional measures are taken in identification and verification of the valid identity and address details of (potential) customers, acceptable to the legal authorities, before performing a transaction and during the course of a continuous business relation.
- ✓ Information should be obtained about whether she/he has political influence, the profession, operated industry and business line from which income is derived within the scope of know your customer principle.
- ✓ Sufficient information and documents should be provided and reasonably investigated in order to confirm sources of funds regarding the customer's transaction.
- ✓ Detailed information should be obtained regarding the duration of the customer's activity and business history in the stated business line.
- ✓ Information should be obtained on the purpose and intended nature of request, which products and services are planned to use and activity volume for the establishment of a continuing business relationship with the Company.
- ✓ Information should be obtained about the geographical location of the place where the activity for the stated business line is performed.
- ✓ Customers and beneficial owners should be checked against the lists which are provided by reputable commercial organizations (such as Dow Jones or World Check) in order to question involvement in known, alleged or suspected financial crime.

4.2. Customer Identification Principles

Identification of customers and verification of the customer's identity within the scope of KYC Principles should be made within the frame of the law and other regulations thereunder. Compliance to KYC Principles which has an important place in FATF recommendations and also adopted by our national laws has crucial importance.

4.2.1. Customer Identification

According to the third part of the "Regulation on Measures Regarding Prevention of Laundering Proceeds of Crime and Financing of Terrorism", which was issued on the date of 09.01.2008 in order to implement the Laws of "Prevention of Laundering of Criminal Proceeds and Terrorism Financing", the principles regarding Customer Due Diligence, 5th clause states that for all transactions made in the Company,

a) Regardless of the monetary amount when establishing permanent business relationships,
b) When the amount of a single transaction or the total amount of multiple linked transactions is equal to or more than seventy five thousand TL,
c) When the amount of a single transaction or the total amount of multiple linked transactions is equal to or more than seven thousand five hundred TL in wire transfers
d) Regardless of the monetary amount in cases requiring STR,
e) Regardless of the monetary amounts in cases where there is suspicion about the adequacy and the accuracy of previously acquired identification information, shall identify their customers or those who act on behalf or for the benefit of their customers by receiving their identification information and verifying it.

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.

4.2.2. Customer identification of natural persons

In customer identification of natural persons, their name, surname, place and date of birth, nationality, type and number of the identity card, address, sample of signature, information on job and profession and, if any, telephone number, fax number, e-mail, and for Turkish citizens, as additional information, the names of mother and father and T.R. identity number shall be received.

Name and surname, place and date of birth, mother's and father's name, nationality, type and number of the identity card of the person concerned shall be verified through;

a) T.R. identity card, T.R. driving license or passport, and identity documents with a Republic of Turkey ID number and clearly stated as official identity documents in special laws for Turkish citizens,
b) Passport, certificate of residence or any type of identity card considered proper by the Ministry for non-Turkish citizens.

After originals or notarized copies of documents which are subject to verification are submitted, their legible phototrcopy or electronic image shall be received or information regarding the identity shall be recorded in order for submittal upon request of authorities.

The address submitted while establishing permanent business relationship shall be verified through Address Registration System or if this information is incomplete or different, a certificate of residence, any utility bill drawn up within the previous three months from the date of transaction for a service requiring subscription such as electricity, water, natural gas, telephone any document issued by a public institution or through any other documents or methods approved by Ministry. Legible photocopies or electronic image of the documents to be verified shall be received or the information specific to them shall be received.

4.2.3. Digital Customer Identification for Natural Persons

In case the related regulation allows the Company to identify and verify customer's identification remotely, digital customer identification methods can be used in order to fullfil customer identification obligation in continous business relation establishment process. Ministry is authorized to determine the methods to be applied during digital customer identification, other measures within Know Your Customer process and other activities to be able to conduct customer idenfication remotely.

4.2.4. Customer identification of legal persons registered to trade registry

In customer identification of legal persons registered to trade registry, the title of the legal person, its trade registry number, tax identity number, field of activity, full address, telephone number, fax number and e-mail, if any, and the name, surname, place and date of birth, ,nationality, type and number of the identity card, and a sample signature of the person authorized to represent the legal person and for Turkish citizens, as additional information, the names of mother and father and T.R. identity number shall be received.

The title of the legal person, its trade registry number, field of activity, full address shall be verified through documents of registration to the trade registry; its tax identity number shall be verified through documents drawn up by the related unit of Revenue Administration.

Identification information of persons authorized to represent the legal person shall be verified through identity cards stipulated in the section of identification of natural persons; and their authority to represent shall be verified through documents of registration.

After originals or notarized copies of documents which are subject to verification are submitted, their legible photocopy or electronic image shall be received or information regarding the identity shall be recorded in order for submittal upon request of authorities.

In establishing permanent business relationship, financial institutions shall verify through consulting records kept by the related trade registry office or the database of Turkish Union of Chambers and Commodity Exchanges whether the information given in registration documents submitted to them are up-to-date and correct.

In case of a request of transaction, within the scope of an existing permanent business relationship, on behalf of the legal person by a written instruction of the person authorized to represent the legal person the authenticity of the identification information of the person authorized to represent the company may be verified through a notarized signature circular comprising the information in identity cards provided that there is no doubt that the instruction is from the representative of the company.

4.2.5. Customer identification of associations and foundations

In customer identification of associations the name of the association, its aim, log number, tax identification number, full address, telephone number, fax number and e-mail, if any, and the name, surname, place and date of birth, nationality, type and number of the identity card and sample signature, and for Turkish citizens, as additional information, the names of mother and father and T.R. identity number of the person authorized to represent the association shall be received. The name, aim, log number and full address of the association shall be verified through the charter of the association and documents of registry in the associations' log; tax identification number shall be verified through documents issued by the relevant unit of the Revenue Administration; the identification information of the person authorized to represent the association shall be verified through identity cards stipulated in the section of identification of natural persons; and the authority to represent shall be verified through documents of authorization to represent.

In customer identification of foundations the name of the foundation, its aim, central registry record number, tax identification number, full address, telephone number, fax number and e-mail address, if any, and the name, surname, place and date of birth, names of mother and father, nationality, type and number of the identity card and sample signature of the person authorized to represent the foundation and for Turkish citizens the additional information as the names of mother and father and T.R. identity number shall be received. The Name, aim, central registry record number, full address of the foundation shall be verified through foundation deed and records kept by the General Directorate of Foundations; tax identification number shall be verified through documents issued by the relevant unit of the Revenue Administration; the identity information of the person authorized to represent the foundation shall be verified through identity cards stipulated in the section of identification of natural persons; and the authority to represent shall be verified through documents of authorization to represent.

Customer identification for branches and representatives of foreign associations and foundations in Turkey shall be conducted depending on registry documents in the Ministry of Interior.

After originals or notarized copies of documents which are subject to verification are submitted, their legible photocopy or electronic image shall be received or information regarding the identity shall be recorded in order for submittal upon request of authorities.

4.2.6. Customer identification of trade unions and confederations

In customer identification of trade unions and confederations the name of the organization, its aim, registry number, tax identification number, full address, telephone number, fax number and e-mail, if any, and the name, surname, place and date of birth, nationality, type and number of the identity card of the person and sample signature of the person authorized to represent the trade unions and confederations and for Turkish citizens the additional information as the names of mother and father and T.R. identity number shall be received. The information gathered shall be verified through charter of these organizations and the records kept by local directorates of Ministry of Family, Labor and Social Security; tax identification number shall be verified through documents issued by the relevant unit of the Revenue Administration; the identity information of the person authorized to represent the organization shall be verified through identity cards stipulated in the section of identification of natural persons; and the authority to represent shall be verified through documents of registration or documents of authorization to represent.

After originals or notarized copies of documents which are subject to verification are submitted, their legible photocopy or electronic image shall be received or information regarding the identity shall be recorded in order for submittal upon request of authorities.

4.2.7. Customer identification of political parties

In the customer identification of political parties, the name of the relevant unit of the political party, its full address, telephone number, fax number and e-mail address, if any, and name, last name, place and date of birth, nationality, type and number of the identity card and sample signature of the person authorized to represent and for Turkish citizens the additional information as the names of mother and father and T.R. identity number shall be received. Name and address of the relevant unit of the political party shall be verified through their charter identity of the person authorized to represent shall be verified through the identity documents stipulated in the section of identification of natural persons, the authority to represent shall be verified through documents of authorization to represent.

After the originals or notarized copies of documents which are subject to verification are submitted, their legible photocopy or electronic image shall be received or information regarding the identity shall be recorded in order for submittal upon request of authorities.

4.2.8. Customer identification of non-resident legal persons and identification on trust agreements established abroad

Customer identification of non-resident legal persons shall be made through copies of the documents approved by the consulates of the Republic of Turkey corresponding to the documents in related country required for legal persons residing in Turkey or through the copies of the documents attached apostille by an authority of the country which is a party to the "Convention on Abolishing the Requirement of Legislation for Foreign Public Documents". Also, in the framework of risk-based approach, when necessary, identity information shall be verified through notarized Turkish translations of copies of the documents.

If a transaction, which requires identification, is requested by a natural or legal person trustee for the asset account of trust agreement established abroad, before these transactions are carried out, a statement including that the request is related to abovementioned agreement has been required at written in accordance with the Article 15 of Law. Identification on trust agreements established abroad shall be verified via trust agreement approved by the consulates of the Republic of Turkey or through the copies of the documents attached apostille by an authority of the country which is a party to the "Convention on Abolishing the Requirement of Legislation for Foreign Public Documents". Also, in the framework of risk-based approach, when necessary, identity information shall be verified through notarized Turkish translations of copies of the documents. Additionally, the documents of the trustee shall be verified through "Customer Identification of Natural Persons" or "Customer Identification of Legal Persons Registered to Trade Registry" part. For the identification of beneficial owner, identity documents of founder, beneficiary or beneficiary groups and the persons assigned as auditor (if any) within the agreement shall be taken and necessary measures shall be taken to verify the documents. Necessary measures shall be taken in order to identify ultimate beneficiaries of the trust agreement.

From the implementation of the abovementioned section, in order to benefit of determined beneficiary or beneficiary group from an asset, trust agreement, it is understood that a legal relationship, ensuring that owner of the asset, founder of the agreement, should assign a trustee that responsible for the management, usage and other disposal of any other properties of mentioned asset included in the agreement, is understood.

4.2.9. Customer identification of unincorporated organizations

In transactions carried out on behalf of unincorporated organizations such as building, housing estate or office block management, the name of the organization, its full address, telephone number, and fax number and e-mail address, if any, and name, last name, place and date of birth, nationality, type and number of the identity document and sample signature of the person authorized to represent the organization and for Turkish citizens the additional information as the names of mother and father and T.R. identity number shall be received. The identity information of the person authorized to represent the organization shall be verified through the identity documents stipulated in the section of identification of natural persons, and the organization information and the authorization of the person acting on behalf of the organization shall be verified through notarized docket.

In customer identification of organizations such as unincorporated joint venture the name of the joint venture, its aim, its full address, telephone number, and fax number and e-mail address, if any, and name, last name, place and date of birth, nationality, type and number of the identity document and sample signature of the person authorized to represent the organization and for Turkish citizens the additional information as the names of mother and father and T.R. identity number shall be received. Information indicating the name, aim, activity field and the address of the partnership shall be verified through notarized partnership agreement, tax identification number shall be verified through the certificates drawn up by the relevant unit of Revenue Administration, identity of persons requesting transaction on behalf of the joint venture shall be verified through identity documents stipulated in the section of identification of natural persons, authorization shall be verified through the documents indicating the authority to represent.

After the originals or notarized copies of documents which are subject to verification are submitted, their legible photocopy or electronic image shall be received or information regarding the identity shall be recorded in order for submittal upon request of authorities.

4.2.10. Customer identification of public institutions

In transactions in which the public administrations in the scope of general administration in accordance with the Public Financial Management and Control Law No. 5018 and quasi public professional organizations are customers, the person making transactions on behalf of these bodies shall be identified in accordance with the section of identification of natural persons. Authorization is verified through the certificate of authority arranged in accordance with the legislation.

4.2.11. Customer identification of those acting on behalf of others

In the event that a transaction is requested on behalf of legal persons or unincorporated organizations by persons who are given the authority by the persons authorized to represent;

a) Customer identification of legal persons and unincorporated organizations shall be carried out in accordance with sections of identification of legal persons registered to trade registry or identification of unincorporated organizations.
b) Customer identification of persons authorized to represent legal persons or unincorporated organizations and the persons who are given the authority by persons authorized to represent shall be carried out in accordance

with the procedure in Article the section of identification of natural persons. In cases where the customer identification of the person authorized to represent cannot be carried out through the identity documents specified in the section of identification of natural persons, the customer identification shall be carried out through power of attorney or circular of signature provided that they contain the information specified in identity documents and that they are notarized.

c) Authorization of persons who are given the authority by the persons authorized to represent shall be verified through notarized proxy or a written instruction of persons authorized to represent. The signatures on the written instruction of persons authorized to represent are verified through their signatures on the notarized circular of signature.

In the event that transactions are made by another person on behalf of a customer that is natural person, customer identification of the person acting on behalf of the customer shall be carried out in accordance with the section of identification of natural persons. Besides, authorization of the person acting on behalf of the customer shall be verified through the notarized power of attorney. In cases where identification of the customer on behalf of whom the act is carried out cannot be conducted in accordance with the section of identification of natural persons, it shall then be conducted through the notarized power of attorney. In the event that the identification of the customer on behalf of whom the act is carried out has already been made due to previous transactions, the requested transaction can be conducted through the written instruction of the customer on behalf of whom the act is carried out provided that the customer's signature on the written instruction is verified through his/her signature which is already available to the obliged party.

In transactions carried out on behalf of minors and persons under legal disability by their legal representatives, 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 event that fathers and mothers request a transaction on behalf of their minor child, it shall be sufficient to identify the child on behalf of whom the transaction is requested and the parent requesting the transaction in accordance with the section of identification of natural persons.

After documents which are subject to verification are submitted, legible photocopy or electronic image of their originals or notarized copies shall be received or information regarding the identity shall be recorded in order for submittal upon request of authorities.

4.2.12. Control of the authenticity of documents subject to verification

Company 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 within the scope of customer identification.

4.2.13. Customer Identification in Subsequent Transactions

In the subsequent face-to-face transactions conducted in the scope of permanent business relationship formerly, identity data shall be received and compared with the data already available to obliged parties. After making comparison, the name and surname of the natural person who is conducting the transaction shall be entered into the related document and his/her sample signature shall be received. In the event that there is suspicion on the authenticity of the data received, these data shall be verified after the submission of identity documents which are subject to verification or of their notarized copies through comparing the data stated on these documents with the data already available to obliged parties. As to the subsequent transactions conducted by using the systems allowing non-face-to-face transactions, necessary measures shall be taken for authentication of the customer and updating the information for customer identification.

4.2.14. Customer identification of those acting for the benefit of others

Company shall be required to take necessary measures in order to detect whether action is carried out for the benefit of another person. Within this scope, obliged parties shall put up required notices in workplaces where they run service in a way that all customers can easily see in order to remind the persons, who act in their own name but for the benefit of others, of their responsibilities. Financial institutions shall also receive, in the establishment of permanent business relationship, the written declaration of the customer indicating whether the act is carried out for the benefit of someone else. This declaration can be specified in the customer contract or be received by using appropriate forms.

In cases where the person requesting the transaction declares that he/she is acting for the benefit of someone else, the identity and the authority 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.

4.2.15. Identification of Beneficial Owner

Necessary measures are taken in order to detect the beneficial owner within the scope of the Know Your Customer Principles.

When establishing permanent business relationship with legal persons registered to trade registry, Company shall identify, in accordance with the section of identification of natural persons., the natural person partners holding more than twenty-five percent of the legal person's shares as the beneficial owner.

In cases where there is a suspicion that the natural person partner holding more than twenty-five percent 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 person(s) detected shall be considered as beneficial owner.

In cases where the beneficial owner is not detected, the natural person(s) holding the position of senior managing official, whose authorization to represent the legal person is/are registered to trade registry, shall be considered as beneficial owner.

Within the scope of permanent business relationship with other legal persons and unincorporated organizations, necessary measures shall be taken in order to detect the natural person(s) who is/are ultimately controlling the legal person. In case where the beneficial owner is not detected, the natural person(s) holding the position of senior managing official within them shall be considered as beneficial owner.

Company must take identity informations of the beneficial owner and must take necessary measures in order to verify the beneficial owner. In this framework, a notarized circular of signature including identity information can be used.

When establishing permanent business relationship with legal persons registered to trade registry, Customer identification process for the legal person partners holding more than twenty-five percent of the legal person shares shall be applied within Customer Identification of Legal Persons Registered to Trade Registry part. Identification documents for non-resident legal persons can be verified through publicly open sources, such as equavalent institution of Turkish Union of Chambers and Commodity Exchanges in the related country.

4.2.16. Transactions requiring special attention

Company shall be required to pay special attention to complex and unusual large transactions and the ones which have no apparent reasonable legitimate and economic purpose, to take necessary measures in order to obtain adequate information on the purpose of the requested transaction, and to keep the information, documents and records obtained in this scope in order for submittal upon request of authorities.

4.2.17. Monitoring the customer profile and the transactions

Company shall be required to follow up permanently the transactions conducted by their customers whether they are in compliance with the information regarding the customer's profession, commercial activities, business history, financial status, risk profile and sources of funds within the scope of permanent business relationships and keep up-to-date information, documents and records regarding the customer. Furthermore, the accuracy of information regarding the telephone and fax number and e-mail address of customers received for customer identification shall be verified, if necessary, within the scope of risk-based approach using these means by contacting with the relevant person. Financial institutions shall also take the necessary measures in order to follow up the transactions conducted out of permanent business relationship in risk-based approach. Financial institutions shall establish, with this purpose, appropriate risk-management systems

4.2.18. Taking measures against technological risks

Financial institutions must pay special attention and take necessary measures, in order to ensure that new and developing technologies, opportunities provided by current and new products and services, including new delivery channels, are not used for the purpose of money laundering and terrorist financing.

The existing products that are restructured as a result of the continuous development of the new services and technology in the Company are checked whether they comply with the laws. The application is followed and the application is stopped when necessary.

Financial institutions are required to take appropriate and effective measures including paying special attention to operations such as permanent business relationship, depositing, withdrawing and wire transfers which are carried out by using method orsystems enabling the institutions to conduct non face-to-face transactions, closely monitoring the transactions that are not consistent with financial profile or activities of the customer or do not have connection with his/her activities, and establishing a limit to amounts and number of transactions.

4.2.19. Reliance on third party

Financial institutions can establish business relationships or carry out transactions by relying on measures taken related to the customer by another financial institution on identification of the customer, the person acting on behalf of customer and the beneficial owner, and on obtaining of information on the purpose of business relationship or transaction. In such a circumstance, the ultimate responsibility shall remain with the financial institution carrying out transaction by relying on the third party under the Law and the related regulations.

Reliance on third parties shall be possible only if it is ensured that; the third parties have taken other 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, the certified copies of documents relating to customer identification shall immediately be provided from the third party when requested.

The financial institution which establishes a business relationship or conducts a transaction by relying on a third party shall immediately receive the identity data of the customer from the third party.

The transactions which the financial institutions conduct between themselves on behalf of customers and relationships between financial institution and its agents, similar units or outsourcing entities are not within the scope of the principle of "reliance on third parties.

The principle of "reliance on third parties" may not be applied to the cases where the third party is resident in a risky country.

4.2.20. Rejection of transaction and termination of business relationship

Company, in cases where they cannot make customer identification or obtain information on the purpose of the business relationship, shall not establish business relationship and not conduct the transaction which they are requested. In such a circumstance they cannot open an anonymous account or account in a fictitious name

In cases where 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. It is also evaluated whether the situations specified situations are suspicious transactions or not.

4.2.21. Correspondent relationship

Financial institutions shall take necessary measures within the framework of risk-based approach in foreign correspondent relationships in order to;

a) Obtain, by making use of publicly available resources, reliable information on whether the respondent financial institution has been subject to a money laundering and terrorist financing investigation and been fined or warned, nature of work, its business field, reputation and the adequacy of supervision on it,
b) Assess anti-money laundering and terrorist financing system of the respondent financial institution and to ascertain that the system is appropriate and effective,
c) Obtain approval from a senior manager before establishing new correspondent relationships,
ç) Clearly determine their and the respondent financial institution's responsibilities by a contract in a way that meets the obligations in Chapter 3 of Regulation On Measures Regarding Prevention Of Laundering Proceeds Of Crime And Financing Of Terrorism,

d) In cases where the correspondent relationship includes the use of payable through account be satisfied that the correspondent financial institution has taken adequate measures pursuant to principles in the Chapter 3 of Regulation On Measures Regarding Prevention Of Laundering Proceeds Of Crime And Financing Of Terrorism and will be able to provide the identification information of the relevant customers when requested.

Financial institutions shall not establish correspondent relationship with shell banks and financial institutions about which they cannot be sure that these institutions do not permit their accounts to be used by shell banks.

For this purpose, Company introduce specific customer acceptance rules, including but not limited to requesting from other financial institutions applying to open correspondent account in the institution, a survey form containing the above given information in writing, and implement specific work flows for which senior management's approval is required.

Sound information is obtained on whether regulatory environment in the country of financial institution with which correspondent banking relation is to be established is at adequate level and investigation is made to determine whether its system related to prevention of money laundering is adequate. An agreement where responsibilities and obligations are set out is made between the finacial group company and the respondent financial institution.

Additional measures regarding the Wolfsberg Anti-Money Laundering Principles for Correspondent Banking may also be considered.

Related practice details and their amendments are determined by procedures, internal regulations and circulars published/will be published by Financial Group AML Department of Bank and Compliance Department of Company.

4.2.22. Wire transfers

It is required that the following information of the originator is included in the cross border and domestic wire transfer messages which amount to seven thousand five hundred TRY or more;

a) Name and surname, title of the legal person registered to trade registry, full name of the other legal persons and unincorporated organizations,
b) Account number or reference number of the transaction where no account number exists,
c) The address or birth of place and date or at least one of the numbers such as TR-ID number, passport number, tax ID number for identifying the originator. Confirmation of this information is required. In wire transfer messages, the information specified in subparagraphs (a) and (b) regarding the recipient is also included, it is not obligatory to confirm this information.

Information specified in subparagraphs (a) and (b) regarding the sender and receiver shall be included in the domestic and international wire transfer messages below seven thousand five hundred TL. Confirmation of this information is not required.

The transfers carried out between the banks on behalf of themselves or for their own benefit and the transfers carried out by using credit or bank cards provided that card numbers are included in the messages shall be out of the scope.

In the event that financial institution receives a wire transfer message not including the information specified in above either it shall return the said wire transfer message or it shall request to complete missing information through the financial institution who sent the message.

In the event that the messages sent include missing information permanently and they may not be completed although they are requested, either the wire transfers received from originator financial institution may be refused or transactions carried out with related financial institution may be restricted or business relationship with related financial institution may be ceased.

In the message chain from the financial institution where the transfer order is given to the financial institution that will make the payment, the information required to be included in the wire transfer messages regarding the sender is included by all financial institutions that mediate the transfer, and special attention is paid to the transfer of this information at every stage of the transfer.

4.2.23. Relationships with risky countries

Financial institutions are required to pay special attention to business relationships and transactions with the natural and legal persons,unincorporated organizations and the citizens located in risky countries and to obtain information about the

purpose and the nature of the transactions, as far as possible, which have no apparent reasonable legitimate and economic purpose and to record them.

The Ministry is authorized to take all necessary measures, including them accepted by international organizations that the Turkey is a member of are considered about risky countries.

4.2.24. Simplified measures

The Ministry of Treasury and Finance may allow financial institutions to take more simplified measures in terms of customer due diligence in the following situations;

a) In transactions carried out between financial institutions on behalf of themselves,
b) In transactions where the customer is a public administration or quasi public professional organization in the scope of general administration in accordance with the 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,
ç) In transactions related to pension schemes that provide retirement benefits to employees by way of deduction from their salaries and of pension agreements
d) In transactions where the customer is a public company and its shares are listed on the stock exchange. The Ministry is authorized to determine applicable measures within the scope of this Article and the transaction types apart from the ones listed above.

However, simplified measures can not apply in cases where money laundering or terrorist financing risks might occur due to the transaction intended to be carried out and shall take into account that the transaction is possibly a suspicious transaction and necessary action should be taken accordingly.

4.2.25. Enhanced measures

Financial institutions shall apply, in proportion to the identified risk, one or more or all of the following enhanced measures for transactions within the scope of articles 18, 20 and 25 of Regulation On Measures Regarding Prevention Of Laundering Proceeds Of Crime And Financing Of Terrorism and for high risk situations they identify in the framework of risk based approach.

a) Obtaining additional information on the customer and updating more regularly the identification data of customer and beneficial owner,
b) Obtaining additional information on the intended nature of the business relationship,
c) Obtaining information, to the extent possible, on the source of the asset subject to transaction and source of funds of the customer,
ç) Obtaining information on the reasons for the transaction,
d) Obtaining approval of senior manager to commence or continue business relationship or carry out transaction,
e) Conducting enhanced monitoring of the business relationship by increasing the number and frequency of the controls applied and by selecting the patterns of transactions that needs further examination,
f) Requiring that in the establishment of permanent relationship the first financial transaction is carried out through another financial institution subject to customer due diligence principles.

The Ministry shall be authorized to determine high risk situations to be taken into account within the scope of this Article and enhanced measures other than ones above.

4.3. Risk Management Activities

Activities related to risk management shall cover at least:

- Developing risk defining, rating, classifying and assessing methods based on customer risk, service risk and country risk,
- Rating and classifying services, transactions and customers depending on risks,
- Developing proper operational and control rules for ensuring monitoring and controlling risky customers, transactions or services; taking necessary measures to reduce risks; reporting in a way that warns related units; carrying out the transaction with ratification of senior authorities and controlling it when necessary,
- Questioning retrospectively the coherency and efficiency of risk defining and assessing methods and risk rating and classifying methods depending upon sample events or previous transactions, reassessing and updating them according to achieved results and new conditions,

- Carrying out required development works through pursuing recommendations, principles, standards and guidelines established by national legislation and international organizations related to issues under the scope of risk,
- Reporting risk monitoring and assessing results regularly to the executive board.

4.3.1. Customer Risk

It includes the risk for obliged parties to be abused due to the business field of the customer allowing intensive cash flow, purchasing of valuable goods or international fund transfers to be carried out easily; and due to the acts of customer or those acting on behalf or for the benefit of the customer for money laundering or financing of terrorism purposes.

For the purpose of grading and reducing the aforementioned risks, individuals or entities with which continuing business relations should not be established as well as additional measures required to be taken are determined by adopting know your customer principles and customer risk profile within the frame of know your customer principle.

4.3.2. Product / Service Risk

Certain products and services are, by their nature, more vulnerable to laundering proceeds of crime, as they facilitate the transfer of funds between different parties. In this context, non-face-to-face transactions, correspondent banking, products and services based on new and developing technologies, safe deposit boxes, prepaid cards, private banking products, and in addition to these, products and services deemed risky in nature within the scope of published procedures are considered within the high risk category.

4.3.3. Country Risk

As a minimum, **countries designated by the Ministry of Treasury and Finance**, which do not have sufficient regulations on the prevention of Money Laundering and the Financing of Terrorism, do not cooperate adequately in combating these crimes, or are deemed risky by authorized international organizations, constitute the country risk.

4.3.4. Risk Categories, Customer Risk Classification and Monitoring Continuosuly

Company determines the risk assessment criteria with a risk-based approach and evaluate the customer, service and country risk together within the specified framework and make a systematic risk rating. In this context, the customer risk classification is created by taking into account the sector in which the customers operate, the profession, the country of citizenship and operation, the frequency of cash usage, the persons / organizations with which they have business relations, the size of their business relationship and the financial services they use. Customer risk classification must be done before starting a business relationship with the customer. The purpose of customer risk classification is to ensure that the risks that the Company may be exposed to are minimized by allowing the customer to be identified, monitoring and control activities.

The risk classification consists of at least 3 categories:

- Low Risk
- Medium Risk
- High Risk

For customers, transactions or services that are classified as high risk, the approval should be obtained of the Compliance Department of Company and, when necessary, the AML Department of Financial Group.

The customer reviews are risk-focused and periodically conducted as specified in the relevant directives.

4.3.5. Additional Measures for High-Risk Groups

One or more or all of the following measures shall be applied in proportion to the risk in order to reduce the risks for customers who are classified as high risk as a result of the risk assessment performed by the Company;

- Obtaining additional information on the customer and updating more regularly the identification data of customer and beneficial owner,
- Obtaining additional information on the intended nature of the business relationship,

- Obtaining information, to the extent possible, on the source of the asset subject to transaction and source of funds of the customer,
- Obtaining information on the reasons for the transaction,
- Obtaining approval of senior manager to commence or continue business relationship or carry out transaction,
- Conducting enhanced monitoring of the business relationship by increasing the number and frequency of the controls applied and by selecting the patterns of transactions that needs further examination,
- Requiring that in the establishment of permanent relationship the first financial transaction is carried out through another financial institution subject to customer due diligence principles.

4.3.6. Individuals and Entities for which Enhanced Measures should be Taken at Establishment of Business Relationship

4.3.6.1. Customer Transactions at Geographical Areas with High Risk Level or Areas Related Thereto

Enhanced measures should be taken to accept as customers individuals/entities that carry out activities in countries that do not cooperate with Financial Action Task Force (of which our country is also a member) or do not have adequate audit mechanisms or individuals/entities that have business relationship with individuals/entities carrying out activities in these countries and continuing business relationship is only established according to enhanced approval mechanism depending on information obtained as a result of reasonable investigation made from external sources

4.3.6.2. Correspondent Banks at Geographical Areas with High Risk Level or Areas Related Thereto

Enhanced measures should be taken to accept as customers individuals/entities that carry out activities in countries outside the EU and countries that do not cooperate with Financial Action Task Force (of which our country is also a member) or do not have adequate audit mechanisms or individuals/entities that have business relationship with individuals/entities carrying out activities in these countries and continuing business relationship is only established according to enhanced approval mechanism depending on information obtained as a result of reasonable investigation made from external sources.

4.3.6.3. Free Zones and Finance Centers

Due care and diligence is exercised with respect to transactions with, free zones and other finance centres that have minimum or no regulatory or audit functions or with respect to customers that have relations with them, and business relationship is established according to enhanced approval mechanism

4.3.6.4. Politically Exposed Persons (PEP) and/or Politically Exposed Persons (PEP) is a Relevant Beneficial Owner of a Client

It is determined whether the customer or beneficial owner is a politically exposed person, a reasonable investigation is made to establish source of funds and wealth and decision to establish business relationship is made according to enhanced approval mechanism.

4.3.6.5. Sensitive Sector and Business Groups

Reasonable investigation should be conducted about individuals or entities which deal in cash transactions intensely or who produce high amounts of cash on specific transactions despite cash disposals not being intense. Decision whether to have a business relation with these individuals or entities or not is made according to enhanced approval mechanism.

Electronic money and payment service business provider companies and virtual currencies providers and exchange platforms are subject to enhanced approval mechanism because of the risks they pose. These organizations must have adapted policies and procedures in compliance with sufficient standards regarding fight against Anti Money Laundering and Terrorist Financing. A detailed investigation on customer basis should be conducted for the customers and final decision will be given by the Compliance Department whether the business relationship will be established or not. The business unit will be able to establish a business relationship by the written approval from their own Senior Management after the positive opinion of the Compliance Department. Approval of AML Department of Main Financial Institution should also be obtained for establishing business relationship.

4.3.7. Individuals, Entities and Countries with Which Business Relationship shall not be Established

4.3.7.1. Individuals and Entities Included in Blacklists Issued by Competent Authorities Within the Scope of Prevention of Laundering of Proceeds of Crime, Financing of Terrorism and Proliferation of Financing Weapons of Mass Destruction Regulations

To establish a business relationship with individuals and entities is forbidden appearing in blacklists issued by competent authorities within the scope of Prevention of Laundering of Proceeds of Crime, Financing of Terrorism and Proliferation of Financing Weapons of Mass Destruction regulations and none of their transactions are effected. In case it is determined that individuals or entities with which business relationship is established have connections with individuals or entities appearing in blacklists, related authorities should be notified. Furthermore, termination of business relationship is also evaluated by Compliance Department.

4.3.7.2. Countries Included in Blacklists Issued by Competent Authorities within the Scope of Prevention of Laundering of Proceeds of Crime and Financing of Terrorism Regulations

Transactions related with sanctioned countries which are given in the blacklists of the competent authorities within the scope of Prevention of Laundering of Proceeds of Crime and Financing of terrorism regulations are not performed.

4.3.7.3. Shell Banks

Direct and indirect transactions and establishing business relationship with shell banks that have no physical presence, are not subjected to any audit and do not have in place adequate regulations on Prevention of Laundering of Proceeds of Crime and Financing of terrorism shall not be permitted.

4.3.7.4. Offshore Banks

Direct or indirect business relationship should not be established with offshore banks that are subject to minimum or no regulatory and supervisory controls, their transactions should not be intermediated.

4.3.7.5. Other Individuals and Entities with Which neither Business Relationship shall not be Established nor Intermediated Transactions

The persons and entities that the Company shall not establish business relationship, including but not limited to the persons and entities mentioned below, are announced to the Company through the procedures and regulations published by the Compliance Department.

- Individuals and entities listed in list of published under Laws 6415 and 7262, local and international sanctioned lists (as a minimum US / OFAC, EU, UN and UK sanction lists) because of involvement and/or convictions in financial crimes, corruption or terrorism.

4.4. Screening of Customers and Payments

All new customers and, where relevant, the directors, beneficial owners and other connected persons are screened against a database that contains:

- the European Union Financial Sanctions List;
- the OFAC SDN List;
- United Nations Security Council List (UNSC);
- 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 Dow Jones or World Check);
- Financial Group'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.

Implementation details and changes related to this issue are identified via internal procedures published/to be published by Financial Group AML Department and Company Compliance Department, circulars and/or procedures.

5. MONITORING AND CONTROL

It is fundamental that the Company should be protected against risks and should be monitored and controlled without interruption to ensure its activities are conducted in compliance with the Law, related regulations, Company's policies and procedures.

Monitoring and Control activities are performed under the responsibility of the 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 conducted by making necessary systemic arrangements and essentially taking into consideration the following issues:

- Monitoring and control of customers and transactions in high risk groups,
- Monitoring and control of transactions with risky countries,
- Monitoring and control of complex and unusual transactions,
- Controlling through sampling method of whether the transactions exceeding the determined amount according to the risk policy are consistent with the customer profile,
- Monitoring and control of connected transactions when taken together that exceed the amount requiring identification,
- Controlling information and documents about customers to be maintained on electronic media or to be maintained in writing and information that is mandatory to be included in electronic transfer messages, rectification of deficiencies and their updating,
- Continuous monitoring throughout the lifetime of the business relation the consistency of the transaction conducted by the customer with information about the business, risk profile and sources of funds of the customer,
- Controlling of transactions conducted by using systems that allow 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 (Article 4.4. Lists specified under Screening of Customers and Payments with Lists) of Competent Authorities within the scope of Prevention of Laundering of Proceeds of Crime and Financing of terrorism.

6. SUSPICIOUS TRANSACTIONS

In case there are any findings, suspicions or grounds for suspicion derived during monitoring and control activities during the performance of non-face to face activities, that the assets involved in the transaction were acquired illicitly or are used for illicit purposes or were used for terrrorist activities or terrorist organizations or by terrorists or by persons financing terrorist activities or are associated with or related to the foregoing, that the customer is conducting transactions inconsistent with its profile, declining to provide information or documents, suspicious transaction reporting is made, regardless of a threshold in amount

In order for the Compliance Officer to fulfill duty in a timely and complete manner, all kinds of support should be provided by the Head Office departments of the Company as well as the branches, representative offices, agencies and / or affiliated units, and the requested information should be conveyed in the desired form and time.

Branches, representation offices, agencies and / or affiliated units and Head Office units of the Company cannot report suspicious transactions directly to MASAK. Suspicious activities should first be directed to the Compliance Department. Transactions that are considered suspicious after the examination should be reported to the Compliance Officer in order to be forwarded to MASAK.

The evaluation of the notifications regarding suspicious transactions will be carried out by the Compliance Department, and the Compliance Officer is authorized to report the transaction to MASAK as a suspicious transaction or not.

Suspicious transaction reports to MASAK within this scope and internal notifications to be made to Compliance Officer cannot be shared with anyone, except related authorities determined by law.

In line with the "Regulation On Postponement Of Transactions Within The Scope Of Prevention Of Laundering Proceeds Of Crime And Financing Of Terrorism" adopted by MASAK on 29 July 2016, if there is any document or serious indication supporting suspicion that the assets which are the subject of a transaction attempted to be conducted or currently going on within or through obliged parties are be linked to offence of laundering or financing of terrorism, obliged parties shall submit a suspicious transaction report (STR) to MASAK with their grounds including the request of suspension of the transaction. This regulation request Banks not make to funds available to the account holder for seven work days and assign responsability for reporting suspicious transaction to MASAK for further investigation.

Notification period of a suspicious transaction to Compliance Officer is at most three working days following the date of detecting the transaction. The period between the date of detecting the suspicious transaction and date of reporting this transaction by Compliance Officer to MASAK is at most 10 working days, including evaluation of Compliance Officer.

7. INTERNAL AUDIT

The internal audit management is responsible to audit annually 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 Company, whether the transactions are carried out in accordance with the regulations and communiqués issued in accordance with the Law and the corporate policy and procedures.

The findings resulting from the internal audit are directed to the Compliance Department, and the necessary measures are taken by the relevant departments to eliminate the deficiencies.

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.

While determining the scope of control, the findings determined during the monitoring and controlling workings and the customers, services and transactions containing risk shall be included within the scope of control.

While determining the units and transactions to be audited, the business size and transaction volume of the Company are taken into consideration. In this context, it is ensured that units and transactions in quantity and quality that can represent all transactions are audited.

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.

8. TRAINING

Company organizes training programs consistent with its size, business volume and other changing circumstances regarding Prevention of Laundering of Proceeds of Crime and Financing of terrorism with the purpose 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.

Training policy of the Company; As a minimum, it is prepared in a way to include issues related to the establishment of corporate policy and procedures of the financial group and Company level, risk management, monitoring and control activities, and information sharing within the group, and training subjects are determined within this scope.

Training activities are conducted under surveillance and coordination of Compliance Officer. Topics for the aforementioned training activities, the employees to participate in the training, the instructors and the annually training schedule are determined jointly by Compliance Officer and Training and Development Group to cover the following subjects at a minimum level and the training program is carried out annually.

At a minimum level, the training subjects are given to the employees include the following;

a) Laundering proceeds of crime end terrorist financing,
b) The stages, methods of laundering proceeds of crime and case studies on this subject,
c) Legislation regarding prevention of laundering proceeds of crime and terrorist financing,
ç) Risk areas,
d) Institutional policy and procedures,
e) In the framework of Law and related legislation;
    1) Principles relating to customer identification,
    2) Principles relating to suspicious transaction reporting,
    3) Obligation of retaining and submitting,
    4) Obligation of providing information and documents,
    5) Sanctions to be implemented in violation of obligations,
f) The international regulations on combating laundering and terrorist financing.

Company's training programs are conducted in two ways- in-class and remote teaching according to experience and job definition of employees to receive training that is prepared by Turkish Banks Association, The Financial Crime Investigation Group. Company must implement and maintain procedures that ensure that training on AML is provided to new joiners within 90 days of their joining. Company shall review the awareness of its employees with periodic surveys or assessments and ensure that employees failing to successfully finish the surveys repeat the training.

The obliged parties shall benefit from training methods such as organization of seminars and panels, constitution of working groups, use of visual and audial materials in training activities, computer-aided training programs working through internet, intranet or extranet etc.

Training covers all of the employees and the instructors must have attended the training of the instructor.

In addition, optional participation in the trainings to be prepared by Koç Holding A.Ş. and open to all employees in the Company will be available.

The training is repeated periodicaly considering also amendments of the regulations and other requirements. The training facilities are controlled by surveys and evaluation processes in terms of the Employees' sufficiency in order to take necessary actions about the results.

Company, relating to the training activities to be implemented, shall report the information and statistics regarding in below to MASAK through the relevant company compliance officer until the end of March of the following year;

a) Training dates,
b) The territory or provinces where training is given,
c) Training method,
ç) Total training hour,
d) The number of staff to whom training is given and the ratio of the staff trained to the total number of staff,
e) Distribution of staff training given according to their unit and title,
f) Content of Training,
g) The title and area of expertise of trainers.

9. REGULATORY TRACKING

Mitigating the Company's potential risk and constantly monitoring and control is important to ensure that activities are conducted in compliance with laws and regulations related to this Law, Corporate Policy and procedures.

Within this scope;

- Company changes to relevant laws, regulations and guidance are identified and analyzed for their impact upon the rules; and make necessary amendments,
- It is ensured that related rules and controls are modified to deal with any material impact of those changes.

10. OBLIGATION TO SUBMIT INFORMATION AND DOCUMENTS

Notifications on Providing Information and documents obligation and information and documents requested by authorized institutions and officers are provided within the frame of the law and regulations thereunder

11. FINANCIAL GROUP INTERNAL INFORMATION SHARING

Companies within the Yapı ve Kredi Bankası Financial Group may share information regarding the account and transactions by knowing the customer in order to ensure that the measures under the compliance program are taken at group level. Written confidentiality provisions in special laws do not apply to information sharing within the group. Those who work in affiliates of the group cannot disclose information regarding knowing customer, accounts and transactions, and cannot use them for the benefit of themselves or third parties. In this context, the sanctions in the relevant laws are applied to those who disclose the information that should be kept confidential. The financial group compliance officer and the board of directors of the main financial institution are also responsible for taking the necessary measures to securely share information within the group. The mentioned responsibility is applicable for both the compliance officers and board of directors of companies within the financial group. The companies within the financial group are not allowed to disclose any information between each other regarding suspicious transaction reports.

12. MAINTENANCE OF RECORDS

Company saves and maintains all information and documents provided to it in accordance with the law on prevention of laundering of proceeds of crime and regulations thereunder in an easily accessible form to be submitted when required and for the duration set out in the legislation.

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.

13. MANAGEMENT INFORMATION AND REPORTING

Compliance Officer ensure that they have appropriate internal management information sufficient to allow them to assess and monitor the Company's risks and effectiveness of controls and that regular reports about the AML programme are made to Senior Management, Audit Committee and Board of Directors. Additionally, in case there is any important issue, necessary reporting is made.

14. OTHER OBLIGATIONS WITHIN THE SCOPE OF PREVENTION OF FINANCING OF TERRORISM AND PREVENTION OF PROLIFERATION OF FINANCING WEAPONS OF MASS DESTRUCTİON REGULATIONS

Company acts in a for the risk-based approach in accordance with the law and the regulations issued under these laws in order to Prevention of Financing of Terrorism and Prevention of Proliferation of Financing Weapons of Mass Destruction.

14.1. Freezing of Asset

Company, shall assure the management of the frozen assets on its records in the framework of the Law No. 6415 on the Prevention of the Financing of Terrorism, Law No. 7262 on the Prevention of Proliferation of Financing Weapons of Mass Destruction and related regulations in accordance with permission of MASAK.

In case of notification and announcement, Company shall inform MASAK of whether they have any asset records, and if they have, of the information on the duly frozen asset within seven days following the date of notification using the same method of notification.

The Company also inform MASAK of the application of unfreezing decisions in accordance with the abovementionned methods of notification. (In seven days following the notification)

14.2. Obligations of the Company

14.2.1. Reporting to MASAK

For freezing any account, Company makes reporting to MASAK the type of business relationship, customer/account number, right and claim.

14.2.2. Blocking Non-Face-to-Face Systems

All credit and bank card of persons, institutions or organizations whose assets are frozen shall be blocked and their access to online banking or all other non-face-to-face systems shall be thwarted by Company.

14.2.3. Freezing Joint Accounts

All of the accounts owned jointly by the third parties and the designated persons, institutions or organizations shall be frozen as a whole by the Company. Other shareholders of frozen accounts shall notify MASAK of their rights on such accounts and the information and documents regarding their basis. The designated persons, institutions or organizations shall pay their debts to other shareholders of joint accounts through the bank account only if MASAK permits so.

14.2.4. Increase in the Amount of the Asset

If there is an increase in the amount of assets frozen, such increase shall also be subject to provisions of the freezing of assets. Therefore, it shall not be possible to access the interest, profit share, dividend and any other revenue to be obtained from the frozen assets except in the cases permitted by MASAK.

14.2.5. Access to Frozen Assets

The power of disposition on frozen assets shall only be exercised upon the permission of MASAK.

Except for the cases permitted by MASAK, those whose assets are frozen may not engage in actions for obliteration, consumption, conversion, transfer, assignation, conveyance and other dispositional actions of the asset. Liable parties shall not allow or facilitate the execution of such actions.

Acts for which Providing or Collecting Funds are Forbidden

Article 3 - It is forbidden to provide or collect funds for perpetration of the following acts:
a) Acts intended to cause death or serious bodily injury for the purpose of intimidating or suppressing a population or compelling a government or an international organization to do or to abstain from doing any act,
b) Acts set forth as terrorist offences within the scope of the Anti Terror Law No.3713 dated 12/04/1991,
c) Acts that are forbidden and stipulated as offence in;
1) Convention for the Suppression of Unlawful Seizure of Aircraft,
2) Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation,
3) Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents,
4) International Convention against the Taking of Hostages,
5) Convention on the Physical Protection of Nuclear Material,
6) Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, Supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation,
7) Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation,
8) Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms Located on the Continental Shelf,
9) International Convention for the Suppression of Terrorist Bombings to which Turkey is a party.

The Offence of the Financing of Terrorism

Article 4 - (1) Any person who provides or collects funds for a terrorist or terrorist organisations 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 within the scope of Article 3 shall be punished by imprisonment for a term of five to ten years, provided that his/her act does not constitute another offence requiring a heavier punishment.
(2) To impose a penalty in accordance with the provision of paragraph one, it shall not be necessary that the funds have actually been used to commit an offence.
(3) In cases where the offences that fall within the scope of this article are committed through undue influence in the public service, punishment to be imposed shall be increased by half.
(4) In cases where the offence is committed within the framework of a legal person's activity, security measures peculiar to legal persons shall be applied.

(5) In cases where the offence is committed against a foreign state or an international organization, investigation or prosecution shall be initiated upon the request of Ministry of Justice.
(6) Provisions of Law No.3713 regarding investigation, prosecution and enforcement shall also apply to this offence.
(7) With regard to this offence, the provisions pertaining to the following measures under the Criminal Procedure Law may apply;
a) Assignment of trustee to company management stated in article 133,
b) Detection of communication, wiretapping and record of communication stated in article135,
c) Assignment of secret investigator stated in article 139,
ç) Tracing by means of technical tools stated in article 140.

15. MONITORING OF CONTROLS

The activities conducted by Company are controlled by Financial Group AML Department whether these activities are conducted in compliance with laws and regulations related to this Law, Corporate Policy and procedures via 2nd Level Controls. This control program is constructed in accordance with the Company's structure.