

	POLICY ON LAUNDERING PROCEEDS OF CRIME AND PREVENTION OF TERRORIST FINANCING	Document No	UYM.PO.05.E
		Release Date	01.08.2023
		Revision No	01
		Revision Date	03.03.2025
		Information Class	Internal Use

POLICY ON LAUNDERING PROCEEDS OF CRIME AND PREVENTION OF TERRORIST FINANCING

Version

1.2

Controlled by

Hülya CİVELEK

Approved by

Sarp TARHANACI

Date

March, 2025

Next Review

March 2026

Table of Contents

1.	PURPOSE	5
2.	SCOPE	5
3.	ABBREVIATIONS AND DEFINITIONS	5
4.	DUTIES, POWERS AND RESPONSIBILITIES	9
4.6.	Duties, Powers and Responsibilities of Board of Directors	9
4.7.	Duties, Powers and Responsibilities of compliance officer	10
4.8.	Resignation of Compliance Officer and Compliance Officer's assistant	11
4.9.	Duties, Powers and Responsibilities of Company personnel	11
5.	KNOW YOUR CUSTOMER PRINCIPLE	12
5.3.	Principles on Knowing Customer	12
5.3.5.	Identification	12
5.3.6.	Identification for Real persons	13
5.3.7.	Remote Identification for Real Persons and Legal persons Registered to Trade Registry	13
5.3.8.	Identification for Legal persons Registered to Trade Registry	14
5.3.9.	Identification for Associations and Foundations	14
5.3.10.	Identification for Trade Unions and Confederations	15
5.3.11.	Identification for Political parties	16
5.3.12.	Identification of Legal Entities Residing Abroad and Trust Agreements Established Abroad	16
5.3.13.	Identification of Unincorporated Organizations	17
5.3.14.	Identification of Public Institutions	17
5.3.15.	Identification of those acting on behalf of a third party	17
5.3.16.	Checking the Authenticity of the Documents Subject to Confirmation	19

5.3.17. Identification in Subsequent Transactions	19
5.3.18. Identification of Those Acting for Third Parties	19
5.3.19. Revealing the Real Beneficiary	20
5.3.20. Actions Requiring Special Attention	20
5.3.21. Monitoring of Customers' Status and Transactions.....	21
5.3.22. Taking Measures Against Technological Risks	21
5.3.23. Trust to Third Party	21
5.3.24. Rejection of Transaction and Termination of Business Relationship.....	22
5.3.25. Correspondent Relationship	22
5.3.26. Electronic Transfers.....	23
5.3.27. Relations with Risky Countries	23
5.3.28. Simplified Measures	24
5.3.29. Tightened Measures.....	24
5.4. Customer Acceptance – General Principles.....	25
5.5. High Risk Customer Acceptance Process.....	25
5.6. Natural and Legal Persons Not to be Accepted as Customers	25
6. RISK MANAGEMENT.....	26
6.1. Risk-Oriented Approach.....	26
6.2. Risk Management Activities	26
6.3. Additional Measures for High-Risk Customer Group	26
7. MONITORING AND CONTROL.....	27
8. TRAINING.....	28
8.1. Training Policy and its Purpose	28

8.2.	Training Activities	28
8.3.	Subjects of Training	29
8.4.	Reporting of Training Results.....	29
9.	INTERNAL AUDIT	30
9.1.	Purpose and Scope of the internal Audit	30
9.2.	Reportingof Internal Audit Activities and Results	30
10.	DETECTION AND REPORTING OF SUSPICIOUS TRANSACTIONS	30
11.	OBLIGATION TO PROVIDE, RETAIN AND SUBMIT INFORMATION AND DOCUMENTS AND CONFIDENTIALITY	32

POLICY ON LAUNDERING CRIME REVENUES AND PREVENTION OF terrorist financing ("Policy") AND PROCEDURES THEREOF

1. PURPOSE

- 1.1. This Policy has been created in order to ensure the necessary compliance with the Law and other relevant legislation in order to prevent Laundering of Proceeds of Crime and terrorist financing in ALEKS METAL RAFİNERİ ANONİM ŞİRKETİ ("Company"). For this purpose, an institutional policy including risk management, monitoring and control, training and internal audit policies has been established within the scope of the Compliance Program, taking into account the size of the business, business volume and the nature of the transactions carried out and taking into account the issues determined within the scope of the national risk assessment.
- 1.2. The purpose of the Policy is to manage the risks in this regard and to provide all kinds of necessary controls by complying with the obligations regarding the prevention of Laundering of Proceeds of Crime and terrorist financing of our Company. At the same time, it is to protect the reputation of the Company, to create a culture of compliance in the institution, to determine the strategies, internal controls, audits and Measures to reduce the risk that the Company may be exposed to, by carrying out all works and transactions with a risk-based approach, to determine the rules of operation, responsibility and relevant responsibilities and to raise awareness of the Company's personnel in this regard.

2. SCOPE

- 2.1. This Policy includes the duties, powers and responsibilities of the Company in the fight against Laundering of Crime Revenues and terrorist financing; regulations within the scope of the principle of knowing the customer it determines; risk management rules determined within the scope of the risk-oriented approach; regulations on monitoring, audit and control; practices on training; issues related to internal audit; detection and notification rules of Suspicious Transactions; regulations on information and document obligation to provide, maintain and submit information and confidentiality.
- 2.2. Within the scope of the policy, issues such as who is responsible for all Measures and operating rules, who or which units are responsible for the approval, realization, reporting and monitoring of transactions according to certain risk limits have been determined and linked to the relevant procedure, process or affiliated document. The second eye rule has formed the basis of duties and authorizations, ensuring that the personnel who will be involved in monitoring, controlling and auditing the company's transactions and workflows according to risks are not also the personnel who perform said transactions.
- 2.3. This Policy covers the Company's board of directors, senior management, authorized signatories, Units, Branches, subsidiaries, affiliates and all managers and personnel at all levels in terms of their duties, powers and responsibilities related to the prevention of Laundering of Crime Revenues and Terrorist Financing.

3. ABBREVIATIONS and DEFINITIONS

Payable Through Account: The type of account opened in a financial institution established in Turkey by a financial institution established in a foreign country within the scope of the correspondence relationship and which also allows the customers of the foreign financial institution to write checks;

Detailed Due Diligence: Detailed customer recognition process developed for risky customers and transactions;

Ministry: Ministry of Treasury and Finance;

Electronic Transfer: The transaction made for the purpose of sending a certain amount of money and securities from a financial institution on behalf of the sender to the recipient in another financial institution by using electronic means;

Financial Institution: The Obligors listed in subparagraphs (a) to (h) and (m) of the first paragraph of Article 4 of the Measures Regulation and the Postal and Telegraph Organization Joint Stock Company (PTT) limited to banking activities;

Certain Non-Financial Jobs and Professions: The Obligors listed in subparagraphs (k), (n), (s), (ş), (t) and (u) of the first paragraph of Article 4 of the Measures Regulation;

Real Beneficiary: The natural person or persons who ultimately control or have ultimate influence over the natural persons who carry out transactions before the obligor, the natural person, legal person or unincorporated entities on whose behalf the transaction is carried out;

Service Risk: The risk that may be exposed within the scope of non-face-to-face transactions, or new products to be offered using developing technologies;

Legal Risk: The possibility of initiating any legal action against a financial institution or adversely affecting the situation or operations of financial institutions due to obligations imposed by contracts or the possibility of financial or reputational damage they may suffer;

The Law: The Law on Prevention of Laundering Proceeds of Crime No: 5549, dated 11/10/2006

Assets: Money, movable or immovable property whose value can be represented by money, all kinds of tangible or intangible goods and rights and all kinds of legal documents or tools that authenticate the rights on them;

MASAK or Presidency: Financial Crimes Investigation Board;

Customer Risk: The risk of abuse of the Obligors due to the fact that the line of business in which the customer operates allows the use of heavy cash, the purchase and sale of high-value goods or the transfer of international funds easily; the customer or those acting on behalf of the customer or on his/her account act for the purpose of Laundering Proceeds of Crime or terrorist financing;

Operational Risk: The possibility of loss arising from inadequate or unsuccessful internal processes, persons and systems or external events, including Legal Risk;

Risk: The possibility of financial or reputational damage incurred by the Obligors or their employees due to the use of the services provided by the Obligors for the purpose of Laundering Crime Revenues or Financing Terrorism or the failure of the Obligors to fully comply with the obligations under the Law and other relevant legislation;

Risky Countries: Countries, those announced by the Ministry from countries that do not have adequate regulations on the prevention of laundering and terrorist financing, do not cooperate in the fight against these crimes or are considered risky by competent international organizations;

Proceeds of Crime: All kinds of economic benefits and values obtained from acts that are considered crimes by the laws according to MASAK. And according to Article 282 of the Turkish Penal Code, this also refers the asset values arising from a crime requires imprisonment 6 months at the lower limit or more.

Laundering Proceeds of Crime: In order to show that the gains obtained illegally as if they have been obtained legally, the transactions aimed at recovering the said gains from in-cash form by entering them into the financial system and gaining legitimacy by changing their identity by going through a process within the financial system;

Continuous Business Relationship: The business relationship established between the company and the customer due to services such as opening an account, issuing a credit or credit card, safe deposit box, financing, factoring, financial leasing, life insurance or individual retirement, which are continuous by nature;

Suspicious Transaction: any transaction possessing any information, suspicion or any consideration requires suspicion indicating that the Asset subject to the transaction made or attempted to be made within or through the Obligors is obtained illegally or used for illegal purposes, is used for terrorist acts or by terrorist organizations, terrorists or those financing terrorism or is related to or connected with them;

Shell Bank: A bank that does not have a physical service office in any country, does not employ full-time personnel and is not subject to the supervision and permission of an official authority in terms of banking transactions and records;

Shell Company: An organization that does not have a physical service office in any country, does not employ full-time personnel and does not have commercial activities;

Measures Regulation: The Regulation on Measures to Prevent Laundering of Proceeds of Crime and terrorist financing published in the Official Gazette dated 9/1/2008 and numbered 26751;

Terrorist financing: Within the scope of Article 3 of the Law No. 6415 on the Prevention of the terrorist financing, all activities of providing and collecting funds to a terrorist individual or terrorist organizations, even without being associated with a certain act, for the purpose of using them in whole or in part or knowingly and willingly;

Compliance Unit: The unit consisting of employees working under the Compliance Officer and responsible for the execution of the Compliance Program;

Compliance Officer: The officer who is employed and equipped with the necessary authority in order to ensure compliance with the obligations imposed by the legislation

enacted on the basis of the Law and the Law;

Compliance Program: The whole of the measures to be created for the prevention of Laundering of Proceeds of Crime and terrorist financing and the scope of which is determined in Article 5 of the Regulation on Compliance Program;

Regulation on the Compliance Program: Regulation on the Compliance Program with Obligations Regarding the Prevention of Laundering of Proceeds of Crime and terrorist financing published in the Official Gazette dated 16/09/2008 and numbered 26999;

Country Risk: The risk that the obligors may be exposed to due to their business relations and transactions with their citizens, companies and financial institutions from countries that do not have adequate regulations on the prevention of laundering and Terrorist Financing, do not cooperate sufficiently in fighting these crimes or are considered risky by authorized international organizations;

Obligor: In the implementation of the Law, refers the companies indicated below and their branches, agencies, representatives and commercial representatives and similar affiliated units: (a) banks, (b) institutions authorized to issue debit or credit cards other than banks, (c) authorized institutions specified in the foreign exchange legislation, (ç) financing and factoring companies, (d) capital market intermediary institutions and portfolio management companies, (e) payment institutions and electronic money institutions, (f) investment trusts, (g) insurance, reinsurance and pension companies and insurance and reinsurance brokers, (ğ) financial leasing companies, (h) institutions providing clearing and custody services within the framework of capital market legislation, (i) Borsa İstanbul Anonim Şirketi, limited to the custody service related to the Precious Metals and Precious Stones Market, (i) Posta ve Telgraf Teşkilatı Anonim Şirketi (Public Postal Service) and cargo companies, (j) asset management companies, (k) precious metals, precious stones and metals, jewelry traders and intermediaries in these transactions, (l) General Directorate of Mint and Stamp Printing, limited to the activity of minting Republic gold coins and Republic jewelry gold, (m) precious metals intermediary institutions, (n) companies engaged in the purchase and sale of immovable property for trade purposes and intermediaries in these transactions (o) companies engaged in the purchase and sale of all kinds of sea, air and land transport vehicles, including construction equipment, and those who mediate these transactions, (ö) those engaged in the purchase and sale of historical artifacts, antiques and artworks or those who auction them, (p) those operating in the field of luck and betting games, including the General Directorate of National Lottery Administration, Turkey Jockey Club and Sports Toto Organization Presidency, (r) sports clubs, (s) notaries, (ş) provided not to violate provisions of other laws in terms of right of defence and except for the information obtained under first paragraph of Article 35 of the Attorneyship Law dated 19/3/1969 and numbered 1136 and due to the professional studies carried out within the scope of alternative dispute resolution methods, independent lawyers, (t) independent accountants, certified public accountants, financial advisors and sworn financial advisors working independently of an employer, (u) independent accountants authorized to audit the financial markets, limited to the realization of financial transactions related to the establishment, merger, management, transfer and liquidation of companies, foundations and associations, audit institutions, (ü) crypto asset service providers, (v) savings financing companies (Branches, agencies, representatives and commercial representatives of the Obligor with headquarters abroad in Turkey and similar affiliated units are considered as Obligors within the scope of the above definition.)

4. DUTIES, AUTHORIZATIONS AND RESPONSIBILITIES

- 4.1. Managers and personnel at all levels of our Company are obliged to fully know our national and international legal and administrative obligations and responsibilities in the fight against Laundering Proceeds of Crime and terrorist financing, and to recognize the regulatory and supervisory institutions involved in the fight. The competent and supervisory institution in the fight against the prevention of Laundering of Proceeds of Crime and the terrorist financing in Turkey is MASAK, which works under the Ministry.
- 4.2. In accordance with the Regulation on the Compliance Program, (a) banks (except for the Central Bank of the Republic of Turkey and development and investment banks), (b) capital market intermediary institutions, (c) insurance and pension companies, (ç) Posta ve Telgraf Teşkilatı Anonim Şirketi (Postal Service) (limited to its banking activities), (d) Group A authorized institutions specified in the Foreign Exchange legislation, (e) Financing, factoring and financial leasing companies, (f) Portfolio management companies, (g) Precious metals intermediary institutions, (ğ) Electronic money institutions, (h) Payment institutions (Exclusively those providing intermediary service for invoice payments, exclusively payment order initiation service and exclusively providing information on the payment account) constitute the Compliance Program. The Compliance Program created covers the branches, agencies, representatives and commercial representatives and similar affiliated overseas units of the Obligor headquartered in Turkey to the extent permitted by the legislation and competent authorities of the country in which they operate. If the legislation of the relevant country does not allow the implementation of the measures within the scope of the Compliance Program, the situation is notified to MASAK and additional measures are taken.
- 4.3. The Compliance Program, which will be established with a risk-based approach in order to ensure the necessary compliance within the scope of the Law and other relevant legislation for the prevention of Laundering of Proceeds of Crime and terrorist financing, includes the following measures.
- a) Establishing company policies and procedures,
 - b) Carrying out risk management activities,
 - c) Conducting monitoring, audit and control activities,
 - ç) Appointment of Compliance Officer and establishment of Compliance Unit,
 - d) Conducting training activities,
 - e) Conducting Internal Audit Activities
- 4.4. Risk management, monitoring and control activities within the scope of the Compliance Program are carried out by the Compliance Officer under the superintendence, supervision and responsibility of the board of directors.
- 4.5. The measures within the scope of the Compliance Program are reviewed at least every two years and necessary updates are made.
- 4.6. **Duties, Powers and Responsibilities of the Board of Directors**
- 4.6.1. The Board of Directors is ultimately responsible for the adequate and effective execution of the Compliance Program in accordance with the scope and characteristics of the

Company within the framework of the Regulation on the Compliance Program. The powers and responsibilities of the Board of Directors are determined as follows within the scope of the relevant regulation;

- a) Appointing a Compliance Officer and a Deputy Compliance Officer,
- b) Determining the powers and responsibilities of the Compliance Officer and the Compliance Unit clearly and in writing,
- c) Approving company policies, annual training programs and changes to be made in them according to developments,
- ç) Evaluating the results of risk management, monitoring and control and internal audit activities carried out within the scope of the Compliance Program,
- d) Taking the necessary measures to eliminate the detected errors and deficiencies in a timely manner,
- e) Ensuring that all activities under the Compliance Program are carried out effectively and in coordination

. The board of directors may delegate some or all of the above powers explicitly and in writing to one or more members of the board of directors residing in Turkey. The transfer of powers in question does not eliminate the responsibility of the board of directors in this regard.

4.7. Duties, Powers and Responsibilities of the Compliance Officer

- 4.7.1. Compliance Officer has been appointed as Compliance Officer in order to establish the standards determined at national and international level in our Company in the fight against Laundering of Proceeds of Crime and terrorist financing and to carry out the Compliance Program. The conditions to be met by the persons to be appointed as Compliance Officer are specified in Article 17 of the Regulation on the Compliance Program. The compliance officer is appointed exclusively as Company personnel, reporting to the board of directors or one or more board members to whom the board of directors delegates its authority. Provided that it is not related to sales and marketing, the Compliance Officer may have other duties that will not disrupt the execution of the Compliance Program.
- 4.7.2. Within the scope of ensuring the necessary communication and coordination with MASAK; The Company's obligation to provide information and documents to MASAK is fulfilled through the Compliance Officer. The Company, from which information and documents are requested, must submit such information and documents to MASAK in accordance with the form and method determined and notified to it.
- 4.7.3. A Compliance Officer Assistant who meets the requirements and qualifications required for the Compliance Officer is appointed for the purpose of conducting the Compliance Program. The Assistant Compliance Officer is appointed exclusively as Company personnel, reporting to the Compliance Officer. The Deputy Compliance Officer shall be appointed in the same period and procedure as the Compliance Officer and the conditions to be met by the persons to be appointed as the Deputy Compliance Officer shall be determined in accordance with Article 17 of the Regulation on the Compliance Program (subject to the exceptions contained in Article 5 of the Provisional Article 1 of the Regulation on the Compliance Program).
- 4.7.4. The Compliance Officer may delegate some or all of his/her duties and powers within the scope of Article 19 of the Regulation on the Compliance Program to the Deputy Compliance Officer explicitly and in writing. The transfer of such duties and powers does not eliminate

the responsibility of the Compliance Officer in this regard. The duties and responsibilities of the Compliance Officer are specified in subclause 1 of Article 19 of the Regulation on the Compliance Program. .

- 4.7.5. The Compliance Officer is obliged to act in good faith, reasonably and honestly, with an impartial and independent will while performing his duties and responsibilities. The Board of Directors ensures that the Compliance Officer has the authority to decide with free will, to request all kinds of information and documents related to his/her field of duty from all units within the Company and to access them in a timely manner.

4.8. **Resignation of the Compliance Officer and the Deputy Compliance Officer**

- 4.8.1. In the event that the Compliance Officer or the Deputy Compliance Officer loses the conditions required by the Regulation on the Compliance Program or it is later understood that he/she does not meet these conditions or leaves his/her duty, the situation shall be notified to MASAK in writing within 10 days from the date of his/her leave from the Company and the new appointment shall be made within thirty days at the latest from the date of leave in accordance with the provisions of Article 16 of the Regulation on the Compliance Program. The commitment form attached to the Regulation on the Compliance Program for Appointment shall be signed by the board of directors or the member or members of the board of directors to whom it has delegated their authority and sent to MASAK within ten days from the date of appointment, taking into account the periods and procedures specified in the Regulation.
- 4.8.2. Until the Compliance Officer is reappointed, the Deputy Compliance Officer shall act in place of him/her.

4.9. **Duties, Powers and Responsibilities of the Compliance Unit**

- 4.9.1. In order to ensure that the Compliance Officer can effectively fulfill his/her duties and responsibilities, the company's board of directors has established a Compliance Unit that is directly affiliated to the Compliance Officer and is responsible for the execution of the Compliance Program and has allocated sufficient personnel and resources to the Compliance Unit.
- 4.9.2. The personnel to be employed in the Compliance Unit may take part in the process of evaluating the internal notifications that may be the subject of Suspicious Transactions in the light of the scope of the Law and other relevant legislation and other information but cannot decide whether to report the transaction to MASAK as a Suspicious Transaction, or cannot report the Suspicious Transaction directly to MASAK. Since the internal notifications made to the Compliance Officer within the scope of the Suspicious Transaction are also subject to confidentiality, the necessary measures for the personnel to work in a way that does not violate this obligation are taken by the Company's board of directors and the Compliance Officer.

4.10. **Duties, Authorities and Responsibilities of Company Personnel**

All personnel of the Company at all levels shall strictly comply with all duties and responsibilities of the Company and its affiliates (subsidiaries) not to be exposed to the risks related to Laundering of Crime Revenues and terrorist financing by implementing this Policy, relevant procedures, relevant documents and Compliance Program appropriately and effectively.

5. KNOW-YOUR-CUSTOMER POLICY

- 5.1. The Company aims to be effectively protected from the risks of Laundering Proceeds of Crime and terrorist financing with the policies, principles and procedures to be regulated in accordance with the legal legislation within the scope of the "KNOW YOUR CUSTOMER" principle.
- 5.2. The principle of "KNOW YOUR CUSTOMER" covers that the Company has sufficient knowledge about the activities of its customers and customers and develops policies and procedures within itself in order to obtain this information. With this policy, it will be ensured to provide clarity in customer transactions and information, to establish and maintain a relationship based on mutual trust, to determine whether the transactions are suspicious according to the legislation and to minimize the risks of the Company.

5.3. Principles Regarding Knowing the Customer

- 5.3.1. Within the scope of the principles regarding the knowing the customer; before the transaction is made from the establishment of the business relationship or the transactions made or mediated by them, the Company is obliged to obtain information about the identity and to determine the identity of those who make transactions by confirming the accuracy of this information and those whose names or accounts are transacted and to take other necessary measures to reveal the Real Beneficiary of the transaction.
- 5.3.2. The documents based on identification are determined by the Ministry and the types of transactions that require identification, their monetary limits and other procedures and principles related to the recognition of the customer are applied within the scope of the Measures Regulation.
- 5.3.3. Identification and know your customer forms prepared according to our procedures will be obtained in real persons and legal entities within the framework of our customer identification rules, and identification forms will be prepared and used by considering other customer identification rules of the Measures Regulation.
- 5.3.4. Our principles regarding customer recognition in accordance with the applicable legislation, policies and procedures within the framework of our rules on Customer Due Diligence are as follows:

5.3.5. Identity Authentication

- a) Our Company,
 - (i) Regardless of the amount in the establishment of the Continuous Business Relationship,
 - (ii) When the transaction amount or the total amount of more than one interconnected transaction is one hundred and eighty-five thousand TRY or more,
 - (iii) When the transaction amount in Electronic Transfers or the total amount of more than one interconnected transaction is fifteen thousand TRY or more,

- (iv) Regardless of the amount in cases requiring Suspicious Transaction notification,
- (v) When there is doubt about the adequacy and accuracy of the previously obtained customer credentials,

must identify its customers and those acting on behalf of or in the name of customers by obtaining the information regarding the identity regardless of the amount and confirm the accuracy of this information and take the necessary measures to reveal the True Beneficiary of the transaction.

- b) Identification is completed before the establishment of the business relationship or before the transaction is completed.
- c) In the establishment of the Continuous Business Relationship, information is obtained about the purpose and nature of the business relationship.

5.3.6. **Identification of Real Persons**

- a) In the identification of real persons; name, surname, place and date of birth, nationality, type and number of identity document, address and signature sample, information about work and profession, telephone number, fax number, e-mail address, if any, and for Turkish citizens, mother's, father's name and Turkish ID number are taken in addition to these information.
- b) The accuracy of the information regarding the name, surname, date of birth, TR identity number and type and number of the identity document of the person concerned are confirmed,
 - (i) through TR identity card, T.R. driver's license or passport and identity documents with T.R. identity number and clearly stated to have official identity in their special laws for Turkish nationals,
 - (ii) through passport, residence document or identity document deemed appropriate by the Ministry for foreign nationals.

. Legible photocopy or electronic image of the original or notarized copies of the identification documents to be submitted by the authorities or information about the identity is recorded.

- c) The accuracy of the address declared in the course of establishment of Continuous Business Relationship is confirmed through certificate of residence, an invoice in connection with a utility requiring subscription such as electricity, natural gas, water, telephone and issued within three months before the date of transaction, or other documents and methods deemed appropriate by MASAK. A legible photocopy or electronic image of the original documents subject to confirmation is taken or the distinguishing information is recorded on the document.
- ç) It is not mandatory to confirm the accuracy of the T.R. ID number in the identification to be made through the TR driver's licenses issued before 1/1/2016.

5.3.7. **Remote Identity Confirmation of Real Persons and Legal Entities Registered in the Trade Registry**

In the event that the Company is allowed to establish a contract with methods that will allow the verification of the identity of the customer without facing the customer in the legislation related to the main field of activity, remote identification methods can be used to verify the customer identity in the establishment of Continuous Business Relations with real persons or legal entities registered in the trade registry. The Ministry is authorized to determine the methods to be applied in remote identification and other measures within the scope of customer recognition and other types of transactions that can be identified remotely by the Obligors.

5.3.8. Legal Entity Identification of Those Registered in the Trade Registry

- a) In the identification of legal entities registered in the trade registry; in addition to the title, trade registry number, tax identification number, field of activity, full address, telephone number, fax number, if any, and e-mail address of the legal entity and the name, surname, place and date of birth, nationality, type and number of the identity document and signature sample of the person authorized to represent the legal entity, mother, father's name and TR ID number are taken for Turkish citizens.
- b) Confirmation of the title, trade registry number, field of activity and address of the legal entity is made through the documents regarding registration in the trade registry; confirmation of the tax identification number is made through the documents issued by the relevant unit of the Revenue Administration.
- c) The accuracy of the identity information of the persons authorized to represent the legal person is confirmed through the identity documents specified in Article 6 of the Measures Regulation and their representation powers are confirmed through the documents regarding registration.
- ç) Legible photocopy or electronic image of the original or notarized copies of the documents to be submitted by the authorities or information about the identity is recorded.
- d) Financial Institutions confirm the up-to-dateness and accuracy of the information contained in the registration documents submitted to them by applying to the relevant trade registry office records or making an inquiry from the database of the Union of Chambers and Commodity Exchanges of Turkey in establishment of the Continuous Business Relationship.
- e) Within the scope of an existing Continuous Business Relationship, if a transaction is requested on behalf of the legal person with the written instruction of the person authorized to represent the legal person, the accuracy of the identity information of the person authorized to represent the company can be confirmed through the notarized circular of signature containing the information in the identity documents, provided that the instruction belongs to the company official.

5.3.9. Identification in Associations and Foundations

- a) In the identification of the associations; information regarding the name, purpose, registry number, tax identification number, full address, telephone number, fax number and e-mail address, if any, of the association, and the name, surname, place and date of birth, nationality, type and number of the identity document and

signature sample and mother's and father's name, and Turkish ID number of the person authorized to represent the association are taken in addition to this information for Turkish citizens. The name, purpose, registry number and address information of the association, the charter of the association and the documents regarding the registration in the registry of the association, the tax identification number, the documents issued by the relevant unit of the Revenue Administration, the accuracy of the identity information of the persons authorized to represent the association, the identity documents specified in Article 6 of the Measures Regulation, and the representation authority are confirmed through the documents indicating that they are authorized to represent.

- b) In the identification of the foundations, the name, purpose, central registration number, tax identification number, full address, telephone number, fax number and e-mail address of the foundation and the name, surname, place and date of birth, nationality, type and number of the identity document of the person authorized to represent and signature sample and mother, father's name and Turkish ID number are taken in addition to this information for Turkish citizens. The name, purpose, central registration number and address information of the Foundation, the articles of foundation and the documents related to the registration kept in the General Directorate of Foundations, the tax identification number, the documents issued by the relevant unit of the Revenue Administration, the accuracy of the identity information of the persons authorized to represent the Foundation, the identity documents specified in Article 6 of the Regulation on Measures, and the representation authority are confirmed through the documents indicating that they are authorized to represent.
- c) Readable photocopy or electronic image of the original or notarized copies of the documents to be submitted by the authorities or information about the identity is recorded.
- ç) Identification of the branches and representative offices of foreign associations and foundations in Turkey is carried out on the basis of the documents related to the registration in the Ministry of Interior.

5.3.10. **Identification in Trade Unions and Confederations**

- a) In the identification of the Trade Unions and confederations, the name, purpose, registration number, tax identification number, full address, telephone number, fax number and e-mail address of these institutions and the name, surname, place and date of birth, nationality, type and number of the identity document of the person authorized to represent the trade union or confederation and signature sample and mother, father's name and Turkish ID number are taken in addition to this information for Turkish citizens. The information received is confirmed through the bylaws of these organizations and other documents based on the registry kept in the regional labor directorates of the Ministry of Family Labor and Social Services, the tax identification number, the documents issued by the relevant unit of the Revenue Administration; the identities of the persons authorized to represent these organizations, the identity documents specified in Article 6 of the Measures Regulation; and the representation authority is confirmed through the documents regarding the registration or the documents indicating that they are authorized to represent.
- b) Readable photocopy or electronic image of the original or notarized copies of the

documents to be submitted by the authorities or information about the identity is recorded.

5.3.11. Identification in Political Parties

- a) In the identification of the political party organization, the name, full address, telephone number, fax number, if any, and e-mail address of the relevant unit of the political party, as well as the name, surname, place and date of birth, nationality, type and number of the identity document and signature sample of the person authorized to represent, and the name of the mother, father and TR ID number are taken in addition to these information for Turkish citizens. The name and address of the relevant unit of the political parties, their bylaws; the identity of the person authorized to represent, the identity documents specified in Article 6 of the Measures Regulation; their status of authority is confirmed through documents indicating that they are authorized to represent.
- b) Readable photocopy or electronic image of the original or notarized copies of the documents to be submitted by the authorities or information about the identity is recorded.

5.3.12. Identification of Legal Entities Residing Abroad and Trust Agreements Established Abroad

- a) Identification of legal entities residing abroad is carried out by observing LBMA /BIST customer acceptance policies and complying with these policies, and the documents corresponding to the documents sought for legal entities residing in Turkey are made on the basis of the samples approved by the consulates of the Republic of Turkey or certified by the authority of the country party to this Convention within the framework of the Convention on the Abolition of the Requirement of Legalization for Foreign Public Documents. In addition, within the framework of the risk-based approach, identity information is confirmed through notarized Turkish translations of these documents when necessary.
- b) In the event that a transaction requiring identification is requested from the Obligors by the real or legal person trustee specified in the contract for the Assets account, which constitutes the subject of a trust agreement established abroad, it must be declared in writing to the Obligors that the transaction is requested for the assets account created within the scope of the trust agreement in accordance with Article 15 of the Law before these transactions are carried out. Identification within the scope of the trust agreement established abroad is made on the basis of written samples of the trust agreement approved by the consulates of the Republic of Turkey or certified by the authority of the country party to this Agreement within the framework of the "Convention on the Abolition of the Requirement of Legalization for Foreign Public Documents". Within the framework of the risk-based approach, identity information is confirmed through notarized Turkish translations of these documents when necessary. In addition, the identity information received within the scope of the identification of the trustee is confirmed in accordance with Article 6 or 7 of the Measures Regulation. As part of determining the Real Beneficiary, the identity information of the contract founder, beneficiary or beneficiary groups and, if any, the persons designated as auditors within the scope of the contract are taken and reasonable measures are applied to confirm this information. Necessary measures are also taken to reveal the real person or persons

who ultimately control the Assets in question.

- c) In the implementation of the above paragraph of the Measures Regulation, the legal relationship stipulating that a certain beneficiary or group of beneficiaries of an Asset be left to the control of a trustee who executes the contract for the purpose of management, use or other dispositions specified in the contract by the contract founder who is the owner of the Asset, is understood.

5.3.13. **Identification in Unincorporated Organizations**

- a) In transactions carried out on behalf of unincorporated entities such as apartment building, building complex, or office building management, the name, full address of the entity, telephone number, fax number and e-mail address, if any, and the name, surname, place and date of birth, nationality, type and number of the identity document of the person authorized to represent the entity and signature sample and mother, father's name and TR ID number are taken in addition to these information for Turkish citizens. The accuracy of the identity information of the person acting on behalf of the organization is confirmed through the identity documents specified in Article 6 of the Measures Regulation; the information of the organization and the authority status of the person acting on behalf of the organization are confirmed through the notarized decision book.
- b) In the identification of the unincorporated joint ventures; information regarding the name, purpose, field of activity, tax identification number, full address, telephone number, fax number and e-mail address, if any, of the joint venture, and the name, surname, place and date of birth, nationality, type and number of the identity document and signature sample and mother's and father's name, and Turkish ID number of the person authorized to represent the joint venture are taken in addition to this information for Turkish citizens. The accuracy of the information regarding the name, purpose, field of activity and address of the joint venture is confirmed through the notarized partnership agreement; the tax identification number, the documents issued by the relevant unit of the Revenue Administration; the identity of the persons requesting transactions on behalf of the joint venture, the identity documents specified in Article 6 of the Measures Regulation; and the authorization status is confirmed through the documents indicating that they are authorized to represent.
- c) Readable photocopy or electronic image of the original or notarized copies of the documents to be submitted by the authorities or information about the identity is recorded.

5.3.14. **Identification in Public Institutions**

According to the Public Financial Management and Control Law No. 5018 ("Law No. 5018"), in transactions where public administrations within the scope of general management and professional organizations in the nature of public institutions are customers, the identity of the person acting on their behalf is determined according to Article 6 of the Regulation on Measures. Authorization status is confirmed over the authorization certificate issued in accordance with the legislation.

5.3.15. **Identification of those acting on behalf of a third party**

5.3.15.1. Necessary identification research should be carried out to determine whether the persons is acting on behalf of a third party. Declarations of the persons are taken in this regard. In the event that the transactions are carried out by another person on behalf of the real person customer, the identity information of the customer and the person acting on behalf of the customer is determined.

- a) In the event that transactions are requested by legal entities or persons authorized by persons authorized to represent them on behalf of unincorporated entities,
 - (i) Identification of legal entities or unincorporated entities shall be carried out in accordance with Articles 7 to 12 of the Measures Regulation.
 - (ii) Identification of the legal person or the persons authorized to represent the unincorporated entity and the person authorized by them shall be made in accordance with the procedure in Article 6 of the Regulation on Measures. If the identification of the person authorized to represent cannot be made through the identity documents in Article 6 of the Measures Regulation, the determination can be made through the power of attorney or signature circular, provided that it includes the information in the identity documents and is notarized.
 - (iii) The authorization status of the persons authorized to represent shall be made through a notarized power of attorney or written instruction given by those authorized to represent. The signatures of the authorized representatives on the written instructions are confirmed by the signatures on their notarized signature circular.
- b) In the event that the transactions are carried out by another person on behalf of the real person customer, the identity of the person acting on behalf of the customer is determined in accordance with Article 6 of the Regulation on Measures. In addition, the authority status of the person acting on behalf of the customer is confirmed through a notarized power of attorney. In the event that the identification of the customer acting on his/her behalf cannot be made in accordance with Article 6 of the Measures Regulation, it shall be made through a notarized power of attorney. In the event that the identity of the customer on behalf of whom the transaction is carried out has been determined due to previous transactions, the requested transaction can be made with the written instruction of the customer on behalf of whom the transaction is carried out, provided that the customer's signature on the written instruction is confirmed by the signature kept at our Company.
- c) In the transactions made by their legal representatives on behalf of minors and constraints, the authority of the guardians and trustees and those appointed by court decision shall be confirmed over the original or notarized copy of the relevant court decision. In the event that parents request a transaction on behalf of their minor children, it is sufficient to determine the identity of the child on whose behalf the transaction is

requested and the parent requesting the transaction according to Article 6 of the Regulation on Measures.

- ç) Readable photocopy or electronic image of the original or notarized copies of the documents to be submitted by the authorities or information about the identity is recorded.

5.3.16. Checking the Authenticity of the Documents Subject to Confirmation

The obligor verifies the authenticity of the document by applying to the person or institution issuing the document or other competent authorities, to the extent possible, in cases where the obligor doubts the authenticity of the documents used for the verification of the information received within the scope of Articles 6 to 14 of the Measures Regulation.

5.3.17. Identification in Subsequent Transactions

In the subsequent transactions carried out face-to-face within the scope of the Permanent Business Relationship of those who have previously been duly identified and require identification, information about the identity is obtained and this information is compared with the information held by the Obligor. After the comparison, the name and surname of the real person who has the relevant document processed are written and a signature sample is taken. If the accuracy of the information received is in doubt, this information shall be verified by comparing the information contained in these documents with the information contained in the Obligor after the submission of the identity documents or their notarized copies. In subsequent transactions that are carried out using systems that enable non-face-to-face transactions and require identification, the necessary measures are taken to verify the identity of the customer and to keep the information within the scope of identification up-to-date.

5.3.18. Identification of Those Acting for Third Parties

5.3.18.1. Necessary identification research should be carried out to determine whether the persons is acting for a third party or not. The statements of the persons are taken in this regard, and in case of suspicion, the necessary research is carried out to reveal the real beneficiary. In the event that the transactions are carried out by another person on behalf of the real person customer, the identity information of the customer and the person acting on behalf of the customer is determined.

- a) Necessary identification research should be carried out to determine whether there is any action made for third parties or not. In this context, in order to remind the responsibilities of the persons acting on their own behalf but for a third party, the necessary announcements are posted as an informative letter in a way that customers can easily see all the workplaces we serve. Financial Institutions also receive a written statement from the client as to whether they are acting for someone else in the establishment of the Permanent Business Relationship. This declaration can be specified in the customer contract or can be obtained using appropriate forms.
- b) When the person requesting the transaction declares that he/she is acting for a third party, the identity and authority status of the person requesting

the transaction and the identity of the person acting for him/her are determined in accordance with Articles 6 to 14 of the Measures Regulation.

- c) If it is suspected that the person is acting on his/her own behalf but for someone else, although he/she declares that he/she is not acting for someone else, measures shall be applied to recognize the Real Beneficiary.

5.3.19. **Revealing the Real Beneficiary**

- a) Necessary measures are taken by the Company to reveal the Real Beneficiary of the transaction.
- b) In the establishment of a Continuous Business Relationship with legal entities registered in the trade registry, the Company determines the identity of the real person partners of the legal entity with a share exceeding twenty-five percent for the determination of the Real Beneficiary in accordance with Article 6 of the Regulation on Measures.
- c) In the event that the real person partner of the legal entity with a share exceeding twenty-five percent is suspected to be not a Real Beneficiary or there is no real person partner with a share at this rate, the necessary measures are taken to reveal the real person or persons who ultimately control the legal entity. The identified real person(s) shall be deemed to be the Real Beneficiary.
- ç) In cases where the Real Beneficiary cannot be determined within the scope of the second and third paragraphs above, the real person or persons with the highest level of enforcement authority registered in the trade registry shall be considered as the Real Beneficiary in the capacity of senior manager.
- d) Within the scope of Continuous Business Relationship, necessary measures are taken to reveal the real person or persons who ultimately control other legal entities and unincorporated entities. In the event that the Real Beneficiary cannot be determined, the real person or persons with the highest executive authority shall be accepted as the Real Beneficiary in the capacity of senior manager.
- e) The identity information of the Real Beneficiary determined within the scope of the above paragraphs is taken and the necessary measures are applied to confirm this information. In this context, notarized circular of signature containing identity information can be used.
- f) In the establishment of a Continuous Business Relationship with legal entities registered in the trade registry, the Company also determines the identity of the legal entity partners who have more than twenty-five percent of the shares of the legal entity in accordance with Article 7 of the Regulation on Measures. Confirmation of the identity information of the legal entity partners residing abroad, which must be obtained in this context, can be made through the open sources of the equivalent organizations of the Union of Chambers and Commodity Exchanges of Turkey in the relevant country or other organizations where the data is officially kept.

5.3.20. **Actions Requiring Special Attention**

Obligors are obliged to pay special attention to complex and unusually large transactions and transactions that do not seem to have a reasonable legal and economic purpose, to take the necessary measures to obtain sufficient information about the purpose of the requested transaction and to keep the information, documents and records obtained in this context available to the authorities when requested.

5.3.21. Monitoring of Customers' Status and Transactions

Obligors are obliged to continuously monitor whether the transactions carried out by their customers are compatible with the information about the profession, business activities, business history, financial status, risk profile and funding sources of their customers within the scope of the Continuous Business Relationship and to keep the information, documents and records about their customers up to date. In addition, the accuracy of the information regarding the telephone and fax number and e-mail address received for the identification of these customers is confirmed by contacting the relevant person using these tools when necessary within the framework of the risk-based approach. Financial Institutions take the necessary measures to monitor the transactions carried out outside the Continuous Business Relationship with a risk-based approach. Financial Institutions establish an appropriate risk management system for these purposes.

5.3.22. Taking Measures Against Technological Risks

- a) Financial Institutions and Certain Non-Financial Businesses and Professions are obliged to pay special attention to the risk of the use of new and developing technologies for the purpose of laundering the opportunities brought by existing and new products and new business practices, including new distribution channels, and to take appropriate measures to prevent this.
- b) The Continuous Business Relationship facility, which is carried out using methods or systems that enable non-face-to-face transactions with Financial Institutions and Certain Non-Financial Businesses and Professions, is obliged to pay special attention to transactions such as account deposits, account withdrawals and Electronic Transfers, to closely monitor transactions that do not comply with the financial profile and activities of the customer or are not related to their activities, and to take appropriate and effective measures, including determining the amount and number of transactions.

5.3.23. Trust to Third Party

- a) Financial Institutions may establish a business relationship or make transactions by relying on the measures taken by another Financial Institution in relation to the customer, in order to determine the identity of the customer, the person acting on behalf of the customer and the Real Beneficiary and to obtain information about the purpose of the business relationship or transaction. In this case, the ultimate responsibility within the scope of the Law and the regulations related to the Law belongs to the Financial Institution that performs the transaction by relying on the third party.
- b) Being able to trust to a third party is only possible provided to be ensured that;
 - (i) The third party has taken other measures to ensure the identification,

storage of records and recognition of the customer, and if it is established abroad, it is also subject to regulations and audits in accordance with international standards in the field of combating laundering and Terrorist Financing,

- (ii) Certified copies of identification documents will be provided immediately from the third party upon request,
- c) The Financial Institution, which establishes a business relationship or makes a transaction by trusting to the third party, immediately obtains the identity information of the customer from the third party.
- d) The transactions made by the Financial Institutions among themselves on behalf of their customers and their relations with the agencies and similar units of the Financial Institutions and the persons to whom they provide services as an extension or complement of the main service units are not within the scope of the principle of trust to the third party.
- e) The trust to third party principle does not apply if the third party is established in Risky Countries.

5.3.24. **Rejection of Transaction and Termination of Business Relationship**

- a) In cases where the company cannot identify itself or cannot obtain sufficient information about the purpose of the business relationship; it does not establish a business relationship and does not perform the requested action. In this context, it cannot open accounts to anonymous or fictitious names.
- b) In the event that the identification and confirmation cannot be made due to doubts about the adequacy and accuracy of the previously obtained customer identity information, the business relationship is terminated.
- c) The Company also evaluates whether the situations specified in the above paragraphs are Suspicious Transactions.

5.3.25. **Correspondent Relationship**

- a) In foreign correspondent relations, Financial Institutions shall take necessary measures;
 - (i) To obtain sound information by using publicly available sources on whether the addressee financial institution has been investigated in terms of laundering or Terrorist Financing and whether it has received penalties or warnings, the nature and subject matter of the work, its reputation and the adequacy of the audit on it,
 - (ii) To evaluate the counter-laundering and counter-terrorism financing system of the addressee financial institution, to ensure that the system is appropriate and effective,
 - (iii) to ensure that the approval of the senior manager is obtained before establishing new correspondent relationships,
 - (iv) To clearly define the responsibilities of themselves and the addressee financial institution with a contract in a way that meets the obligations in Article 5 titled Know Your Customer Principle,

- (v) In cases where the correspondent relationship covers the use of Relayed Correspondent Accounts, to ensure that the addressee financial institution has taken adequate measures within the framework of the principles in Article 5 titled Know Your Customer Policy and can provide the identity information of the relevant customers when requested
- b) Financial Institutions cannot enter into correspondent relationships with Shell Banks and financial institutions that they are not sure that they do not make their accounts available to Shell Banks.

5.3.26. **Electronic Transfers**

- a) In domestic and international Electronic Transfer messages of fifteen thousand TRY or more, following information of the sender must be indicated;
 - (i) Name and surname, title of the legal entity registered in the trade registry, full name of other legal entities and unincorporated entities,
 - (ii) Account number, in case the account number is not available, the reference number related to the transaction,
 - (iii) At least one of the information used to identify the sender, such as address or place and date of birth or customer number, citizenship number, passport number, tax identification number

and the accuracy of this information is also confirmed. Electronic Transfer messages include the information specified in subparagraphs (i) and (ii) above regarding the recipient, and it is not mandatory to confirm this information.

- b) Domestic and international Electronic Transfer messages below fifteen thousand TRY include the information specified in subparagraphs (i) and (ii) above regarding the sender and the recipient. Confirmation of this information is not mandatory.
- c) Transfers using credit and debit cards are outside the scope of paragraph (a), provided that card numbers are used in messages.
- d) The Financial Institution receiving an Electronic Transfer message that does not contain the information specified in paragraph (a) above shall return the said Electronic Transfer or ensure the completion of the missing information from the Financial Institution sending this message.
- e) In the event that the messages sent constantly contain incomplete information and this information is not completed on request, the receiving Financial Institution shall consider the rejection of Electronic Transfers from the sending Financial Institution or the restriction of transactions with the said Financial Institution or the termination of the business relationship.
- f) In the message chain formed from the Financial Institution where the transfer order is given to the Financial Institution that will make the payment, all the information that should be included in the Electronic Transfer messages regarding the sender is included by all Financial Institutions that mediate the transfer and special attention is paid to transfer this information at every stage of the transfer.

5.3.27. **Relations with Risky Countries**

5.3.27.1. Financial Institutions and Certain Non-Financial Businesses and Professions must pay special attention to the business relations and transactions they will enter with natural and legal persons, unincorporated entities and citizens of these countries located in Risky Countries, collect and record information as much as possible about the purpose and nature of the transactions that do not have a seemingly reasonable legal and economic purpose.

5.3.27.2. The Ministry is authorized to determine the measures to be taken regarding the Risky Countries, including those accepted by the international organizations to which Turkey is a member.

5.3.28. **Simplified Measures**

a) By the Ministry,

- (i) In the transactions carried out by Financial Institutions among themselves,
- (ii) In transactions where the customer is a public administration or a professional organization in the nature of a public institution within the scope of general management according to Law No. 5018,
- (iii) In the establishment of a business relationship through collective customer acceptance within the scope of the salary payment agreement,
- (iv) In transactions related to pension plans and pension contracts that provide pension rights to employees by deducting their wages,
- (v) In transactions where the customer is a publicly traded company and its shares are listed on the stock exchange,

the Obligors may be allowed to take simpler measures in terms of measures for the recognition of the customer. The Ministry is authorized to determine the types of transactions other than those listed above with the measures that can be applied within the scope of this article.

b) In cases where there may be a risk of laundering or Financing of Terrorism due to the transaction, the obligors cannot apply simplified measures and take into account that the transaction may be a Suspicious Transaction according to Article 27 of the Measures Regulation.

5.3.29. **Tightened Measures**

a) In high-risk situations to be determined within the framework of the transactions within the scope of Articles 18, 20 and 25 and the risk-based approach in the Regulation on Measures for Financial Institutions and Certain Non-Financial Businesses and Professions, it applies one or more or all of the following measures in proportion to the identified risk.

- (i) To obtain additional information about the customer and to update the identity information of the customer and the Real Beneficiary more frequently.
- (ii) To obtain additional information about the nature of the business relationship.
- (iii) To obtain as much information as possible about the source of the Assets subject to the transaction and the funds belonging to the customer.

- (iv) To obtain information about the purpose of the transaction.
 - (v) To make the entering into a business relationship, the continuation of the existing business relationship or the realization of the transaction subject to the approval of the senior officer.
 - (vi) To increase the number and frequency of the controls imposed and to keep the business relationship under strict supervision by determining the types of transactions that require additional control.
 - (vii) To require that the first financial movement in the establishment of the Continuous Business Relationship be made from another Financial Institution to which the principles of customer recognition apply.
- b) The Ministry is authorized to determine high-risk situations to be taken into account within the scope of what is specified herein and also tightened measures other than those listed above.

5.4. Customer Acceptance – General Principles

5.4.1. In relation to this Policy, our Company shall take the necessary measures to be informed at least on the following;

- a) Determination of real identity and address,
- b) Consistency of documents and information within itself,
- c) The customer's profession, the main business subject that generates income, the principles of his/her business,
- d) The customer's transaction profile and capacity, workplace or place of activity.

5.4.2. During the acceptance of new customers through all kinds of channels, the Company personnel is responsible for determining the identity and address of the customers, providing all kinds of information and documents, verifying this information and reflecting it in the Company processes, as stipulated by the relevant legal legislation and in accordance with the internal legislation and practices of our Company.

5.5. High Risk Customer Acceptance Process

Establishing a business relationship with high-risk customers is submitted to the approval of the senior officer, and it is aimed to directly identify, control and reduce risks through managerial controls and internal control activities. Supervision is carried out regarding the effectiveness of functions such as compliance, risk management, quality, security, financial controls and internal control processes. Internal audit activities, on the other hand, aim to provide assurance on the effectiveness of risk management and control processes as an independent party with a risk-based approach.

5.6. Natural and Legal Persons Not to be Accepted as Customers

- a) Those who refrain from providing information and documents;
- b) Those who want to open an account with an anonymous name or nickname;
- c) Those who refrain from providing information about their transactions and the source of their money;
- d) Those on the sanctions list of OFAC, the European Union, and similar international organizations and countries, or on the list of those whose assets are frozen, those on the list of those wanted for terrorism;
- e) Shell Banks or Shell Companies

- f) Illegal gamblers and bettors;
- g) Those who engage in fraudulent activities with methods such as pyramid sales system, Ponzi scheme, network marketing;
- h) Those engaged in alternative transfer system (hawala) activities,

They are not accepted as customers by the company.

6. RISK MANAGEMENT

6.1. Risk-Oriented Approach

- 6.1.1. Within the scope of this Policy, the obligors establish a risk management policy by considering the size of the business, business volumes and the nature of the transactions they carry out. With a risk-oriented approach, our Company carries out an effective struggle to identify, rate, monitor, evaluate and reduce the risks it may be exposed to.
- 6.1.2. The risk management policy covers the internal measures and operating rules regarding the measures in the "Principles Regarding the Recognition of the Customer" section of the Measures Regulation at a minimum level.

6.2. Risk Management Activities

- a) Risk management activities covers the following activities at a minimum level;
 - (i) Developing methods of identification, rating, classification and evaluation of risks based on Customer Risk, Service Risk and Country Risk, taking into account national and international standards,
 - (ii) Rating and classification of services, transactions and customers according to risks,
 - (iii) Ensuring the monitoring and control of risky customers, transactions or services; taking necessary measures to reduce risks; reporting in a way that warns the relevant units; developing appropriate operation and control rules for the transaction to be carried out with the approval of the senior authority and audited when necessary,
 - (iv) Questioning the consistency and effectiveness of risk identification and evaluation methods, risk rating and classification methods retrospectively through case studies or transactions, to re-evaluate and update them according to the conclusions and developing conditions,
 - (v) Carrying out the necessary development studies by following the national legislation and the recommendations, principles, standards and guidelines brought by international organizations regarding the issues within the scope of risk
 - (vi) Reporting the results of risk monitoring and evaluation to the board of directors at regular intervals

6.3. Additional Measures for High-Risk Customer Group

- 6.3.1. The Company shall apply one or more or all of the following measures in proportion to the identified risk in order to reduce the risk to be undertaken for the groups determined as high-risk as a result of the risk rating;

- a) To obtain additional information about the customer and to update the identity information of the customer and the Real Beneficiary more frequently,
- b) To obtain additional information about the nature of the business relationship,
- c) To obtain as much information as possible about the source of the assets subject to the transaction and the funds belonging to the customer,
- d) To obtain information about the purpose of the transaction,
- e) To make the entering into a business relationship, the continuation of the existing business relationship or the realization of the transaction subject to the approval of the senior officer,
- f) To carry out Detailed Due Diligence if necessary, in relations with politically influential persons and to take them to the compliance committee for approval,
- g) Conducting Detailed Due Diligence for high-risk customers if necessary, taking them to the compliance committee for approval,
- h) To increase the number and frequency of the controls imposed and to keep the business relationship under strict supervision by determining the types of transactions that require additional control.
- i) To require that the first financial movement in the establishment of the Continuous Business Relationship be made from another Financial Institution where the principles regarding the recognition of the customer are applied,
- j) To pay special attention to the transactions of natural or legal persons residing in Risky Countries,
- k) To make a detailed examination about the purpose and nature of transactions that do not have a seemingly reasonable, legal and economic purpose,
- l) To visit high-risk corporate customers on-site.

6.3.2. The Ministry is authorized to determine high-risk situations to be considered within the scope of this section and also tightened measures other than those listed above.

7. MONITORING AND CONTROL

- 7.1. Within the scope of this Policy, the Company carries out monitoring and control activities by considering the size of the business, the business volume and the nature of the transactions it performs. The purpose of monitoring and control is to protect the Company from risks and to continuously monitor and control whether its activities are carried out in accordance with the applicable legislation and the Company's policies and procedures.
- 7.2. Monitoring and control activities are carried out by the Compliance Officer under the supervision, supervision and responsibility of the board of directors within the framework of the Regulation on the Compliance Program and the provisions of this Policy.
- 7.3. Within the scope of monitoring and control activities; the deficiencies detected as a result of the controls carried out in order to ensure compliance with the obligations imposed in accordance with the Law are reported to the relevant units in order to take the necessary measures and the results are followed up.
- 7.4. Within the framework of monitoring and control activities, the Company is obliged to ensure that the personnel who will carry out these activities have access to internal information sources.
- 7.5. Monitoring and control activities covers following activities at a minimum level;

- a) Monitoring and control of customers and transactions in the high-risk group,
- b) Monitoring and control of transactions with Risky Countries,
- c) Monitoring and control of complex and unusual transactions,
- d) Checking whether the transactions above an amount to be determined by the Obligor according to the risk policy are compatible with the customer profile by sampling method,
- e) Monitoring and control of linked transactions exceeding the amount that requires identification, when considered together,
- f) Checking the information and documents about the customer that are supposed to be kept electronically or in writing, and the information that is supposed to be included in electronic transfer messages, completing any deficiencies, and updating them
- g) Continuously monitoring whether the transaction carried out by the customer is compatible with the customer's business, risk profile and funding sources throughout the business relationship,
- h) Controlling the transactions performed using systems that enable non-face-to-face transactions,
- i) Controlling services that could become vulnerable to abuse due to newly introduced products and technological developments using a risk-oriented approach.

8. TRAINING

8.1. Training Policy and its Purpose

- 8.1.1. Within the scope of this Policy, our Company creates a training policy that will include issues such as the functioning of training activities, who will be responsible for their realization, the determination, training and training methods of the personnel and trainers who will participate in the training activities.
- 8.1.2. While organizing training activities on fighting Laundering Proceeds of Crime and Terrorist Financing, our Company aims to understand and adopt the risks of Laundering Proceeds of Crime and Terrorist Financing by the Company's personnel, to create a corporate culture, to increase the awareness of responsibility for risk reduction activities and to keep the information of the personnel up-to-date, and to ensure compliance with the obligations imposed by laws and regulations.
- 8.1.3. The purpose of the training policy is to ensure compliance with the obligations imposed by the Law and the regulations and communiqués issued in accordance with the Law, to create a corporate culture by increasing the awareness of the personnel on the Company policy and procedures and risk-based approach, and to update the information of the personnel.

8.2. Training Activities

- 8.2.1. Obligors are obliged to carry out training activities in accordance with business sizes, business volumes and changing conditions in order to prevent Laundering of Proceeds of Crime and Terrorist Financing.
- 8.2.2. Training activities are carried out under the supervision and coordination of the Compliance Officer. The company carries out its training activities in a way that includes the following subjects and within the annual training program. The training program is prepared by the Compliance Officer with the participation of the relevant units. Effective

implementation of the training program is overseen by the Compliance Officer.

8.2.3. Training activities are reviewed with the participation of the relevant units according to the results of the assessment and evaluation and are repeated at regular intervals according to the need, at least once a year.

8.2.4. In order to ensure the spread of company training activities throughout the company, training methods such as organizing seminars and panels, forming working groups, using visual and audio materials in training activities, computer-aided training programs working over the internet, intranet or extranet, e-learning programs can be used.

8.3. **Subjects of Training**

8.3.1. The trainings to be given to the personnel by the company shall include following subjects in a minimum level;

- a) The concepts of Laundering Proceeds of Crime and Terrorist Financing,
- b) Stages and methods of Laundering Proceeds of Crime case studies on this subject,
- c) Legislation on prevention of Laundering Proceeds of Crime and Financing of Terrorism,
- d) Risk Areas,
- e) Company policy and procedures,
- f) Within the framework of the law and the relevant legislation;
 - (i) Principles regarding the recognition of the customer,
 - (ii) Principles regarding Suspicious Transaction notification,
 - (iii) Obligation of retention and submission
 - (iv) Obligation of providing information and documents
 - (v) Sanctions to be applied in case of non-compliance with the obligations,
- g) International regulations in the field of fighting money laundering and terrorist financing,

8.3.2. The training content can be differentiated in accordance with the purpose based on the duration, title and duty of the personnel in the Company and it is ensured that each personnel receives all trainings regularly in accordance with the relevant legislation.

8.4. **Reporting of Training Results**

8.4.1. Regarding the training activities implemented, the information on;

- a) Training Dates:
- b) Regions or provinces where education is provided,
- c) Training Method,
- d) Total Training Hours,
- e) The number of personnel trained and their percentage to the total number of personnel,
- f) Distribution of the trained personnel according to their units and titles,
- g) The content of the training,
- h) The title and areas of expertise of the trainers,

is reported by the company to MASAK through the Compliance Officer by the end of March of the following year.

9. INTERNAL AUDIT

9.1. Purpose and Scope of the Internal Audit

- 9.1.1. The purpose of the internal audit is to provide assurance to the Board of Directors on the effectiveness and adequacy of the Compliance Program as a whole.
- 9.1.2. The Company ensures that its policies and procedures, risk management, monitoring and control activities and training activities are sufficient and efficient, the adequacy and effectiveness of the Company's risk policy, whether the transactions are carried out in accordance with the regulations and communiqués issued in accordance with the Law and the Company's policies and procedures are examined and audited annually with a risk-based approach.
- 9.1.3. The internal audit activities of the Obligors within the scope of the Compliance Program are carried out by the internal audit unit. The personnel to be authorized to carry out internal audit activities must not have received duties and authority in the fulfillment of other measures within the scope of the Compliance Program in order to ensure that they work independently.

9.2. Reporting of Internal Audit Activities and Results

- 9.2.1. The deficiencies, errors and abuses revealed as a result of the internal audit and the opinions and suggestions to prevent their reappearance are reported to the Company's board of directors.
- 9.2.2. When determining the scope of the audit, customers, services and transactions that contain disruptions and risks detected in monitoring and control studies are included in the scope of the audit.
- 9.2.3. When determining the units and transactions to be audited, the Company's business size, organizational structure, business and transaction volume are taken into account. In this context, it is ensured that the units and transactions in quantity and quality that can represent all the transactions carried out by the Company are audited.
- 9.2.4. Regarding the works carried out within the scope of the internal audit activity; the information and statistics required within the framework of the legislation regarding the internal audit activities carried out, including the annual transaction volume of the Obligor, the total number of personnel and the total number of branches, agencies and similar affiliated units, the number of branches, agencies and similar units audited, the dates of the audits carried out in these units, the total audit period, the personnel employed in the audit and the number of transactions audited, are regularly kept and reported to MASAK by the Compliance Officer until the end of March of the following year.

10. DETECTION AND REPORTING OF SUSPICIOUS TRANSACTIONS

- 10.1. Suspicious Transaction; It is the presence of any information, suspicion or suspicion that the assets subject to the transaction made or attempted to be made within or through the Company are obtained illegally or used for illegal purposes, for terrorist acts within this scope, or used by terrorist organizations, terrorists or those who finance terrorism or that they are related or connected to them.

- 10.2. Suspicious Transactions are notified to MASAK by the Company Compliance Officer within 10 (ten) business days at the latest from the date of suspicion of the transaction, regardless of the amount, by completing the Suspicious Transaction Notification Form, taking into account the information and findings obtained by investigating the transaction, if necessary, to the extent of their powers and possibilities.
- 10.3. The issue of whether there is a reasonable reason for doubt or suspicion is evaluated by considering multiple transactions together when necessary. The fact that Suspicious Transactions have been reported within the scope of continuous information does not eliminate the obligation to report Suspicious Transactions. MASAK is authorized to determine suspicious transaction types.
- 10.4. In addition, in accordance with our international certificates, all Suspicious Transactions non-compliance notifications are collected at the Company Compliance Officer, evaluated and forwarded to the relevant places according to LBMA and BIST procedures.
- 10.5. If new information and findings are obtained later regarding the notified transaction, the Suspicious Transaction Notification Form is filled again and sent to MASAK without delay, stating that it is an annex to the previous notification.
- 10.6. The Company cannot not provide information to anyone else on that a Suspicious Transaction has been or will be notified to MASAK, including those who are parties to the transaction, except for the information given to the auditors assigned with the obligation audit and to the courts during the trial. This obligation includes the persons, institutions and organizations that report the Suspicious Transaction to MASAK or the members of these persons who actually carry out and manage the transaction or their legal representatives and attorneys, as well as other personnel who are in any way aware that a Suspicious Transaction has been reported. Internal notifications to the Compliance Officer are also confidential. Compliance Officers who perform Suspicious Transaction notifications electronically cannot give cards, passwords and other information and tools in all kinds of environments that provide access to the system to anyone. The company shall not disclose their head offices, branches, agencies, representatives, commercial proxies and similar affiliated units abroad any information that they have reported a suspicious transaction in relation to their customers. Natural and legal persons who fulfill the obligation to notify Suspicious Transactions, their Compliance Officers, legal representatives, managers and employees of the Obligors cannot be held responsible for legal and criminal aspects in any way.
- 10.7. If there are critical documents or signs supporting the suspicion that the Assets subject to the attempted or ongoing transaction are related to the crime of laundering or Financing of Terrorism, the suspicious Transaction notification is sent to MASAK with the request for postponement of the transaction with its reasons and the realization of the transaction is avoided for the period specified in the legislation.
- 10.8. In instant notifications from the Refinitiv World Check One screening software regarding the freezing of assets:
- a) All transactions are frozen by notifying the Accounting Department immediately, and added to the List of Frozen and Unemployed Companies in the Compliance Department Customer and Supplier Account numbers;
 - b) The trial balance of the relevant company is requested from the Accounting

- Department;
- c) In any case, all transactions are notified in accordance with the legal legislation, even if the transaction has been made in the past or has been encountered in new registration scans within the scope of the Customer or the Supplier;
 - d) If the decision to freeze assets is about our Company or our Company's board of directors, authorized signatories or directors, the actions to be taken are carried out in accordance with MASAK's "Practice Guide on Freezing Assets" published in 2022.
- 10.9. Suspicious Transaction notification obligation is carried out in accordance with the legal legislation.

11. OBLIGATION TO PROVIDE, RETAIN AND SUBMIT INFORMATION AND DOCUMENTS AND CONFIDENTIALITY

- 11.1. The Company is obliged to notify MASAK of the transactions to which it is a party or which it mediates, exceeding the amount to be determined by the Ministry. Transactions that are interrelated in nature are considered as a single transaction. Transactions made on weekends and holidays and during the night are considered to be transactions of the first business day following the time when these transactions are made. In the provision of continuous information by the Company to MASAK, the transactions carried out by the banks on their own behalf and accounts and the transactions carried out by the Financial Institutions with the administrations within the scope of general management, public economic enterprises and professional organizations in the nature of public institutions in accordance with the Law No. 5018 are not falling under the obligation to provide continuous information.
- 11.2. According to the Law on the Prevention of Laundering Proceeds of Crime and the legislation based on it, all information, documents and records that must be received and kept regarding customers and transactions are kept within the framework of the periods and principles specified in accordance with the legislation. For the avoidance of doubt, all personal data processed by the Company during the activities, works and transactions of the Company within the scope of the Law on the Protection of Personal Data No. 6698 ("PDPL") and the relevant legislation applications shall be stored and destroyed in accordance with the PDPL and other relevant legislation and the policies prepared by the Company in this context.
- 11.3. The company is obliged to retain the documents related to its obligations and transactions in all kinds of environments for a period of eight years from their date of issue, from the date of last registration for the books and records, and from the date of last transaction for the documents and records related to identification, and to submit them to the authorities if requested. The start date of the retention period of the documents related to the identification of the accounts with the obligor is the date the account is closed.
- 11.4. The documents and records for the Suspicious Transaction notification made to MASAK or internal notifications made to the Compliance Officer, the documents attached to the notification, the written reasons for the Suspicious Transactions decided not to notify by the Compliance Officers are within the scope of the retention and submission obligation.
- 11.5. Within the scope of the obligations to provide information / documents and to provide continuous information, the requests are fulfilled in accordance with all kinds of applicable legislation. The confidentiality of information, documents and records related to customers

and transactions is complied with and kept in accordance with all kinds of applicable legislation and for the period stipulated within the scope of this legislation, and it is destroyed appropriately when the said period expires.

Sarp TARHANACI
Chairman of The BoD