Turkish Financial Crimes Investigation Board (MASAK)

Main Principles Regarding the Prevention of Money Laundering and Financing of Terrorism

For Crypto Asset Service Providers

May 2021

A. BRIEF INFORMATION ON MASAK AND ITS ACTIVITIES

MASAK started its operations on 17 February 1997 as per Law No. 4208 of Anti Money Laundering, following its entry into force on 19 November 1996.

Subsequently, MASAK's mandate has been re-established with Law No. 5549 on the Prevention of Laundering of the Proceeds of Crimes and Presidential Decrees No. 1 and 43.

The main functions of MASAK are conducting research and sectoral studies, development of prevention mechanisms, collection of data, analysis and evaluation of collected data, and sharing the information and results of such activities with the relevant authorities regarding the prevention of money laundering and the financing of terrorism.

B. THE CRIME OF MONEY LAUNDERING

Money laundering is a crime under Article 282 of Turkish Criminal Code, which stipulates that "*If a person conducts the following acts in relation to an asset value, which has been acquired as a result of a crime for which the minimum required period of imprisonment is six months or more, shall be sentenced to* ***imprisonment for a term of three to seven years and a judicial fine up to twenty thousand days****: transferring such asset abroad, making various transactions to give the impression that such asset was legitimately acquired or concealing its illegitimate source. Moreover, a person who purchases, accepts, keeps or uses an asset value subject to this crime without aiding and abetting shall be sentenced to* ***imprisonment for a term of two to five years***."

Based on this, the crime of laundering involves the following:

For an act to constitute money laundering, a prior crime that generates an income has to be committed.

- First, a crime must be committed. This crime must be defined under the Turkish Criminal Code for which a minimum six months of imprisonment must be envisaged (e.g. dealing drugs, forgery in official or private documents, theft or robbery). An economic value must be acquired as a result of this crime, i.e. proceeds of a crime which is defined as any economic gain and value acquired through acts deemed to be criminal by law.
- Lastly, some actions must be taken to make the assets seem as if they were acquired through a legal source (e.g. any act or transaction aiming to conceal the source of the proceeds of a crime or give the impression that they were legally acquired, such as transferring the assets abroad).

C. THE CRIME OF FINANCING OF TERRORISM

Financing of terrorism is a crime under Article 4 of Law No. 6415, which stipulates that "*a person who provides or raises funds for a terrorist or a terrorist organization for the funds to be partially or completely used in criminal acts defined under Article 3 (hereunder), or with intention to be used in such criminal act, even without a connection to such criminal act, shall be* ***imprisonment for a term of five to ten years*** *unless it constitutes a heavier crime*."

The sentence stipulated for the financing of terrorism is imprisonment for a term of 5 to 10 years unless such acts constitute a heavier crime.

While the primary aim of terrorists and terrorist organizations is not to acquire assets, they do need to find financial sources in order to fund their activities.

As proceeds acquired through illegal means can lead to financing of terrorism, proceeds acquired through legal sources may also cause this crime.

These sources may be summarized as follows:

Subscriptions and donations: *Those who are not members of or associated with a terrorist organization may provide financial contributions to terrorist organizations voluntarily or due to fear. These donations and contributions may be directly in cash or through the provision of food, medication, equipment etc.*

Through non-profit organizations: *Financing of terrorism may be achieved through funds raisedby non-profit organizations. Those who donate mostly do not know their funds will be sent to terrorist organizations and make such financial contributions in good faith, assuming that their funds will be used for the legal means manifested by these organizations.*

Proceeds acquired through publications: *Aside from using them to spread their ideologies and to provide theorical training for their supporters, terrorist organizations acquire proceeds by selling newspapers, magazines and books to their supporters.*

External support: *Over the course of history, terrorism has been a tool in foreign policy, directly or indirectly used by some countries (considered to be a necessity for national and international politics). External support plays a great role in the growth of terrorist organizations. It is difficult for a terrorist organization to maintain its activities and have food, shelter, training, guns etc. solely from internal sources and without any external support. Countries that support terrorist organizations help themby granting asylum to their members, allowing them to establish subsidiaries such as associations and*

media organizations within their territory, donating weapons and ammunition, and providing logistical support such as shelter, clothing and food.

Commercial Activities: *Terrorist organizations may also be supported by transferring legal commercial proceeds and establishing entities run by terrorist organization members, ex-members or those who give the impression that they are not related to the financing of terrorism.*

Social events: *Terrorist organizations may collect large amounts of money by organizing social events such as concerts, feasts, exhibitions and shows.*

Drug Smuggling: *Drugs, which are easy to produce, easy to transfer, easy to exchange in return for cash, and have high demand, are an important source of income for terrorist organizations.*

Demanding A Ransom: *Kidnapping people and asking for a ransom is one of the sources of financing terrorism. When a terrorist organization proves its success in these activities, it can continue to receive funds using only scare tactics and threats.*

Collecting "Tax": *Terrorist organizations often collect money through threats or in return for protection or for causing no harm. Sometimes, they forcibly collect money from people under the name of "tax".*

Forgery: *Today's printing technology and the easy access to all kinds of printing tools, equipment and materials required for printing, have allowed terrorist organizations to specialize in forgery. These organizations print counterfeit money and fake passports. While they primarily print fake passports and identity cards for their own members, they also earn income by printing fake passports for criminal organizations upon request.*

Human Trafficking: *Terrorist organizations, which are closely linked with illegal immigration organizations, both earn income and recruit new members through human trafficking.*

Apart from these sources, illegal acts such as fraud, robbery, extortion, and theft are also used to finance terrorism.

D. THE DUTY-BEARERS

In order to prevent money laundering and the financing of terrorism, to ensure efficiency in combatting these crimes and to prevent the use of the financial system by criminals, certain "Duty-Bearers" have been determined in law and various duties have been imposed on them.

Financial and non-financial institutions, which are defined as Duty-Bearers, as well as some categories of businesses and occupations may be used as intermediaries by criminals due to their fields of activity and the services they provide. In other words, the transactions and services provided by the Duty-Bearers can be used by criminals to commit crimes. Duty-Bearers should play a "preventive" function in combatting the crimes of money laundering and the financing of terrorism and to achieve this function, they should be made aware of these crimes. Duty-Bearers are the most important partners of the Financial CrimesInvestigation Board in combatting crime.

Duty-Bearers are specified in Article 2/1-d ofthe Law on the Prevention of Laundering Proceeds of Crimes (Law no. 5549) and Article 4/1 of the Regulation on Measures for the Prevention of Money Laundering and Terrorism Financing (the "Regulation").

Crypto Asset Service Providers have been added to the list of Duty-Bearers as of 01 May 2021 in paragraph (ü) of Article 4 of the Regulation with the amendment published in the Official Gazette on the same date (Official Gazette no. 31471).

Crypto Assets are intangible assets that are created virtually using a distributed ledger or a similar technology and distributed over digital networks but are not qualified as tokens, deposit money, electronic money, payment instrument, security or other capital market instruments. Crypto Asset Service Providers are the intermediaries that enable purchases and sales of Crypto Assets through their electronic transaction platforms.

In the Regulation on the Non-Use of Crypto Assets in Payments published by the Turkish Central Bank, Crypto Asset is defined as *"intangible assets that are created virtually using a distributed ledger or a similar technology and distributed over digital networks but are not qualified as tokens, deposit money, electronic money, payment instrument, security or other capital market instruments*." Crypto Asset Service Providers are the intermediaries that enable purchases and sales of Crypto Assets through their electronic transaction platforms.

E. OBLIGATIONS

The obligations of Duty-Bearers are stipulated under Articles 3 and 9/A of the Law on the Prevention of Laundering Proceeds of Crimes (Law no. 5549) while the details of these obligations are included in relevant regulations and communiques.

On this basis, the obligations of Crypto Asset Service Providers are (1) customer identification, (2) reporting suspicious transactions, (3) providing information and documents, (4) periodic reporting, and (5) retention and submission of documents.

1. Obligation to Identify Customers

According to Article 3 of Law number 5549 Duty-Bearers must **confirm the identities** of customers making a transaction (or persons on whose behalf a transaction is made) on their platform and to take other necessary measures **before a transaction** is made.

Detailed regulations on customer identification are found in Articles 5 and 26/A of the Regulation. The most important precautionary measure in scope of customer identification is “confirmation of identity”. In the Regulation transactions that require confirmation of identity are classified as (i) those that depend on the transaction amount and (ii) those that do not depend on the transaction amount.

As Crypto Asset Service Providers and users enter into contracts and the subsequent transactions are carried out within the scope of user memberships based on these contracts, this constitutes a "**continuous business relationship**". Therefore, it is necessary for Crypto Asset Service Providers to obtain user identity information and verify this information when finalizing a contract, **regardless of the amount of the transaction**.

Apart from continuous business relationships, Crypto Asset Service Providers must confirm the identity of users in the following cases:

- In cases that require suspicious transaction reporting, regardless of the amount,,
- in cases that involve suspicion on the adequacy and accuracyof the previously obtained customer identification information, regardless of the amount,
- When a single transaction amount or the total amount of multiple related transactions are TRY 75,000 or more.

Identification processes must be completed before entering into a contract (establishing a business relationship) or making a transaction.

a. Obligation to Identify Individuals

Identification of individuals is stipulated under Article 6 of the Regulation, which sets forth (i) the information to be obtained under the obligation, (ii) the information that must be verified, and (iii) the documents that serve as the basis for this verification.

Information to be obtained: Name, surname, birthplace and date, nationality, type and number of identity documents, address and signature sample, information about their profession, telephone number (if any), fax number (if any), e-mail address (if any), and additionally, parents' names and T.R. identification number for Turkish citizens.

Information to be verified: The accuracy of an individual's name, surname, date of birth, T.R. identification number (for Turkish citizens), and the type and number of identity documents must be verified based on the following:

For Turkish citizens: T.R. ID card, T.R. driver's license or passport and other identity documents that contain a T.R. identification number and are accepted as official identity documents in law.

For foreigners: Passport, residence document or identity document approved by the Ministry.

Approved identity documents can be found on the official website at https://masak.hmb.gov.tr/sikca-sorulan-sorular.

After the original or notarized copies of identity documents subjected to verification are submitted to the Duty-Bearer, they must make a **legible photocopy**, a **digital copy** or record the identity information, which are to be forwarded to the authorities when requested.

The accuracy of an address declared in a permanent business relationship must be verified through (i) a residency certificate, (ii) an invoice under the individual's name related to a subscription-based service such as electricity, water, gas, or telephone issued within three months of the transaction or (iii) other documents and methods deemed appropriate by MASAK. More information on documents and methods approved by MASAK are found on

the official website at https://masak.hmb.gov.tr/sikca-sorulan-sorular. Again, the Duty-Bearer must make a **legible photocopy**, a **digital copy** or record the relevant information.

b. Obligation to Identify Businesses

Identification of legal entities registered under the trade registry is stipulated under Article 7 of the Regulation, which sets forth (i) the information to be obtained under the obligation, (ii) the information that must be verified, and (iii) the documents that serve as the basis for this verification.

Information to be obtained: The legal entity's title, trade registry number, tax identification number, field of activity, address, telephone number, fax number (if any) and e-mail address (if any). Name, surname, place and date of birth, nationality, type and number of the identity document of the legal entity's authorized representative along with parent'snames and their T.R. identity numbers if they are Turkish citizens.

Information to be verified: Verification of the legal entity's title, trade registry number, field of activity and address must be made through trade registry records. The verification of the tax identification number must be made through documents issued by the relevant tax authority.

The identity information of persons authorized to represent the legal entity must be verified through the identity documents required for individuals, and their authority to represent the legal entity must be verified through trade registry documents.

After the original or notarized copies of the identity documents subjected to verification are submitted to the Duty-Bearer, it must make a **legible photocopy**, a **digital copy** or record the identity information, which are to be forwarded to the authorities when requested.

Identification of legal entities residing abroad must be made through the corresponding documents required for legal entities residing in Turkey, which are either approved by the consulates of the Republic of Turkey or confirmed with an annotation by the foreign authority within the framework of the Apostille Convention. In addition, as per the risk-based approach, identity information may be verified through notarized Turkish translations of these documents when required.

Customer identification obligations regarding other types of customers such as associations, foundations, unions, confederations, political parties, unincorporated organizations, public institutions, and those acting on behalf of someone else are found in Articles 8 through 17 of the Regulation.

c. Identification in Consecutive Transactions

According to Article 16 of the Regulation, in consecutive transactions (face-to-face and requiring identification) that are made within the scope of a permanent business relationship, by those individuals who have been duly identified before, the identity information submitted by the individual must be compared with the information in the Duty-Bearer's records. Following the comparison, the name and surname of the individual must be recorded on the relevant document and a signature sample must be taken. In the case of suspicionabout the accuracy of the information received, a verification must be made after the individual submits original documents or notarized copies proving the information by comparing them to the Duty-Bearer's records.

In consecutive transactions that require identification and that are carried out using systems thatenable non-face-to-face transactions, necessary measures must be taken to verify the identityof the customer and to keep such information up to date.

Consecutive transactions of TRY 75,000 or more made by customers who have established a permanent business relationship by signing a membership agreement with Crypto Asset Service Providers, will be considered as consecutive transactions.

How is identification performed in cases where Crypto Asset Service Providers do not come face-to-face with the customer / user?

The identification methods for individuals and legal entities above correspond to situations in which a Duty-Bearer and a customer are face-to-face. In cases where Crypto Asset Service Providers do not come face-to-face with their customers, they can fulfill their identification obligations through couriers and external support units (support service organizations). Couriers and external support units cannot be considered third parties as they act on behalf of Crypto Asset Service Providers. They should be considered as the personnel who assist Crypto Asset Service Providers in the proper performance of the identification obligation. **Therefore, the relevant Crypto Asset Service Providers are responsible for the procedures undertaken by couriers and external support units.** Crypto Asset Service

Providers must enter into contracts with these couriers and external support units to receive their services. The subject and scope of the support service and the responsibilities of the parties must be clearly and understandably stated in a contract. In determining the scope of the agreement, the provisions of the "Regulation on Supporting Services for Banks" published by the Banking Regulation and Supervision Agency and the chapter titled "Operation Principles of Investment Institutions" of the "Communique on the Establishment of Investment Institutions" published by the Capital Markets Board can provide guidance.

On the other hand, it is possible for Crypto Asset Service Providers that exclusively operate electronically to benefit from simplified procedures if they fulfill the conditions specified in the Article 2.2.10 of the Financial Crimes Investigation Board General Communique No. 5. These conditions include an agreement with a bank residing in Turkey regarding electronic transactions, and verification of identity information through the Ministry ofInternal Affairs' General Directorate of Population and Citizenship Affairs database.

d. Declining Transactions and Termination of Business Relationships

Declining transactions and the termination of business relationships are stipulated under Article22 of the Regulation. As per this provision, in cases where identification cannot be made or sufficient information cannot be obtained regarding the purpose of the business relationship,the business relationship cannot be established, and the requested transaction cannot be made.

In cases where identity information cannot be verified following a suspicion on the adequacy andaccuracy of the information, the business relationship must be terminated. Whether this constitutes a suspicious transaction must be evaluated separately.

2. Obligation to Report Suspicious Transactions

There are two approaches to combating money laundering and financing of terrorist crimes. The first involves deterrent measures aimed at investigating, examining and revealing a crime,the perpetrators, and the proceeds of the crime.

The second and more important approach is the set of activities called "preventive measures" aimed at preventing money laundering and financing terrorism before a crime takes place.

Suspicious transaction reporting is one of the most important elements of combatting money laundering and financing terrorism. Suspicious transaction reporting aims at detecting and

preventing money laundering and financing terrorism through cooperation between Duty-Bearers and MASAK. A suspicious transaction is defined in Article 4/1 of Law No. 5549 and Article 27/1 of the Regulation, and the procedures and principles of suspicious transaction reporting are regulated under Articles 27 to 30 of the Regulation and MASAK General Communique No. 13.

It is sufficient to have "information", "suspicion" or "a matter that raises suspicion" for a suspicious transaction to occur.

A suspicious transaction is a situation in which there is “information”, “suspicion” or “a matter that raises suspicion” that assets subject to a transaction made or attempted before or through Duty-Bearers have been obtained illegally, used for illegal purposes, used for terrorist acts or by terrorist organizations and terrorists or terrorist financiers.

"Suspicion" refers to a subjective state of mind that will occur in those who carry out and/or intermediate a transaction within which the funds or assets may have been obtained from illegal sources or may be used for an illegal purpose.

A Duty-Bearer should evaluate a suspicion according to its perception and intuition, the behavior of the customer during the transaction, the information previously obtained about the customer, the compatibility of the transaction and transaction amount with the financial profile of the customer and other factors.

When a suspicious transaction is encountered, a Duty-Bearer must report it to MASAK by filling out the **Suspicious Transaction Reporting Form** as per the information and evidence it obtained to the extent possible.

Suspicious transactions are reported to MASAK, regardless of the transaction amount. **Reporting suspicious transactions within the scope of periodic reporting does not eliminate the obligation to report suspicious transactions.**

- The term "transaction" in the term suspicious transaction is not limited to a single transaction, and can include more than one transaction.

- A single Suspicious Transaction Reporting Form must be completed for transactions thatraise suspicion when multiple transactions are considered together.

Suspicious transaction reporting should not be confused with reporting a crime. MASAK is an administrative body and the suspicious transaction reports it receives are used in determining the validity of a Duty-Bearer's suspicion, and no action is taken for suspicious transaction reports that cannot be linked to money laundering and financing terrorism crimes. From thefirst stage to the last stage of the reporting, the sender of the suspicious transaction report isnever disclosed. During the suspicion analysis stage, which is conducted in full confidentiality,if it is found that the suspicion is based on concrete evidence only then the file is submitted tothe judicial authorities with the relevant evidence, information and documents, and again, without specifying who made the initial reporting of the suspicious transaction.

Suspicious transaction reporting also prevents the Duty-Bearers from the possibility of participation on these crimes due to the business relationship they have established with persons who are involved or thought to be involved in money laundering and financing terrorism.

a. Who Reports Suspicious Transactions?

The obligation to report suspicious transactions is fulfilled by the legal representatives of a Duty-Bearer.

The legal representatives are responsible for evaluating the information and findings obtained through their investigations, to the extent possible within their power, and reporting the transactions they deem to be suspicious to MASAK.

Suspicious transaction reporting can be made by filling in the suspicious transaction report form (found at https://masak.hmb.gov.tr/sektorel-sib-rehberleri) and submitting a physical copy in person or via registered mail to MASAK. If a suspicious transaction reportis sent to MASAK by fax, the original form must also be sent by registered mail or submitted in person. Signed letters sent to MASAK without filling in the form are not accepted as a suspicious transaction report.

It is also possible to send suspicious transaction reports electronically. Electronic suspicious transaction reporting is made through the EMIS.ONLINE system, which Duty-Bearers can accessvia https://online.masak.gov.tr.

To access the EMIS.ONLINE system, a "Suspicious Transaction Reporting in Electronic Environment" form should be prepared by the legal representative of the Crypto Asset Service

Provider and submitted to MASAK. The authorization document for the legal representative must also be sent along with the form.

Subsequently, a user account will be created in the EMIS.ONLINE system for the legal representative, and the password required to access this account will be automatically sent to the business e- mail address of the legal representative. The legal representative will change their password when they first access the EMIS.ONLINE system.

Suspicious transactions must be reported to MASAK within ten business days from thedate of suspicion at the latest.

In cases where the legal representatives of a Duty-Bearer changes, a "Suspicious Transaction Reporting in Electronic Environment" form must be completed and sent to MASAK again for the newly authorized legal representative.

b. When Should Suspicious Transactions Be Reported?

Suspicious transactions must be reported to MASAK **within 10 business days from the date a suspicion is raised** at the latest. **Cases that are delayed may cause harm, suspicious transactions must be immediately reported.**

c. What Kinds of Transactions May Be Suspicious?

Make sure to check out the Suspicious Transaction Reporting Guide at masak.hmb.gov.tr/sektorel-sib-rehberleri

Based on the definition of a suspicious transaction, finding out "**information**" about transactions and customers based on press or similar sources undoubtedly requires reporting. The real question is how to determine the existence of "**suspicion**" or "**a matter that raises suspicion**".

Suspicious transactions are discovered beginning with any behavior that may raise suspicion in an average person while being supported by a Duty-Bearer's knowledge, experience, and professional responsibility.

In this context, the types of suspicious transactions in the "Sectoral Suspicious Transaction Reporting Guidelines" on the official website of MASAK are presented as a guide for Duty-Bearers but Duty-Bearers should not limit themselves to these examples. Even if a suspicious transaction does not fit any of the types listed, Duty-Bearers must report transactions they deem suspicious.

d. Matters To Be Considered When Reporting Suspicious Transactions

During the reporting process, a Duty-Bearer may need to conduct a detailed investigation, to the extent possible within its power, about the nature of a transaction or a customer profile. The purpose of an investigation is to determine whether there are additional findings that will support a suspicion. While conducting the investigation, attitudes and behavior that will cause the customer to suspect the reporting process should be avoided.

In cases that require suspicious transaction reporting, the necessary identification procedures should be performed by Duty-Bearers. However, in cases where the suspicious transaction subject to reporting remains at the stage of an attempt and has not been carried out, the obligation to identify must still be fulfilled to the extent possible.

Duty-Bearers cannot disclose suspicious transaction reporting to anyone, including thosewho are party to a transaction, except for the relevant official auditors and the courts during trials.

Violators are subject to imprisonment for one to three years and a judicial fine of up to 5000 days.

3. Obligation to Provide Information and Documents

According to Article 7 of Law No. 5549; public institutions, real and legal persons, and organizations without legal entity status are responsible for providing all kinds of information, documents, and records in all mediums requested by MASAK and its inspectors, including providing all information and passwords required to access records or to make themreadable.

The aforementioned responsible parties cannot avoid providing information and documents by way of resorting to provisions of special laws, without prejudice to the provisions regardingthe right to defense.

While investigating suspicious transactions, attitudes and behavior that may raise suspicion in the customer should be avoided.

4. Obligation to Retain and Submit Documents

According to Article 8 of Law No. 5549; Duty-Bearers are obliged to keep documents regarding obligations and transactions **for eight years** from the date of issuance, the books and records from the last record date, and documents

related to identification from the date of the last transaction and submit them to the authorities if requested.

Crypto Asset Service Providers are obliged to periodically report information within the framework of the procedures and principles to be determined by the Ministry.

5. Obligation to Report Periodically

According to Article 6 of Law No. 5549, Duty-Bearers are obliged to notify MASAK of transactions, which they are a party to or mediate, exceeding an amount to be determined by the Ministry.

The types of transactions, the procedure and duration, Duty-Bearers who are exempt, and other procedures and principles regarding the obligation of periodic reporting are to be determinedby the Ministry.

F. SANCTIONS

Violations found as a result of audits carried out as per the first paragraph of Article 13 ofLaw No. 5549 regarding the obligations to identify customers, periodic reporting, and to report suspicious transactions will result in administrative fines imposed by MASAK **per transaction** in the amounts specified in law.

The total amount of the administrative fine to be applied cannot exceed a certain amount for each obligation within the same year. In cases of a violation of the same obligation in the following year by a Duty-Bearer who had been fined on the upper limit previously, such limits will be doubled for the following year.

In this context, pursuant to the amendments to Article 13 of Law No. 7262 and Law No. 5549, the following administrative fines, and upper limits apply to violations in 2021.

Obligation	Administrative Fine for a Single Violation (TRY)	Administrative Fine Upper Limit (TRY)
Identifying Customers	30,000	4,000,000
Reporting Suspicious Transactions	50,000	4,000,000
Periodic Reporting	30,000	4,000,000

According to paragraph 7 of Article 17 of the Misdemeanor Law No. 5326, administrative fines increase every year based on the revaluation rate determined and announced as per Article 298 of the Tax Procedure Law No. 213, effective from the beginning of each calendar year.

Pursuant to Article 14 of Law No. 5549, imprisonment of one to three years and a judicial fine of 5,000 days will be imposed on Duty-Bearers that violate (i) the obligation not to disclose suspicious transaction reporting to anyone except official auditors and judicial authorities, (ii) the obligation to provide information and documents, and (iii) the obligation to retainand submit documents. Specific security measures will be imposed on legal entities with regard to this crime.

G. EXAMPLES OF SUSPICIOUS TRANSACTIONS

Examples Related to Customer Profile
Insufficient or contradictory information in the documents submitted, or reluctance to provide information during the application process.
Offering money or various gifts to proceed with the application or negative news in the media regarding money laundering or financing of terrorism.
Behavior that falls outside of general customer behavioral patterns such as adopting a very close or a threatening attitude at times to prevent reporting suspicious transactions.
Lack of a reasonable balance between a customer's job, financial situation, and their transactions.
Commercial or other relationships with risky persons or organizations.
Companies having an unusual capital, partnership, management, or employment structure compared to other organizations in the sector of activity or in general.
Examples Related to Transactions
No repetition of transactions that are usually repeated in commercial life, or on the contrary, repetition of transactions that are not frequently performed in ordinary commercial life.

Dividing financial transactions usually made in bulk without a reasonable justification.
Lack of common sense and reasonable legal or economic justification for a transaction.
Unusual use of payment tools, such as making a large cash payment with small billsor wanting to pay with a currency that is not frequently used.
General Examples Related to Transactions
Customer asking questions in an attempt to gather information about identification procedures and suspicious transaction reporting, transaction limits, the methods of combatting money laundering.
Difficulty in obtaining personal information from a customer such as area of activity, profession, address or telephone number.
A customer having difficulty in explaining the purpose of a transaction or the source of the fund subject to the transaction or refraining from providing such information.
A customer trying to persuade personnel not to present or fill in a required document.
Different customers providing the same address, telephone and similar contact information.
Remarkable and excessive cash transactions or electronic transfer traffic directed from withinor outside the country observed in the accounts of persons who do not have foreign relatives or business relationships and who have opened a joint time deposit account.
Unusual transfer frequency from domestic and foreign accounts to a joint account of individuals who are not relatives and do not have a business relationship.
New dominant shareholder(s) of legal entity customers refraining from giving information about their personal and commercial backgrounds, showing signs that they have no interest, education or work experience in the field in which the company operates.

Customers attempting to proceed with names that are suspected to be fake and without submitting official identity documents.
Proposals, pressure or threats to personnel to block them from reporting suspicious transactions.
Examples Related to People with Suspected Connections to Terrorist Organizations orTransactions With Risk Countries
Performing transactions or opening an account before a Duty-Bearer on behalf of real andlegal person known to be linked to a terrorist organization.
Electronic transfers and/or withdrawals to commercial accounts opened in risky countries without a valid commercial explanation or economic purpose.
Sending and/or receiving funds from risky countries, opening accounts in financial institutionsin these countries or using credit cards issued by banks in these countries.
Transferring funds to countries where terrorism and smuggling are prevalent or that are known tax havens in which a customer has no apparent business connection.
Transferring funds from risky countries to third parties in short periods of time.
Collecting funds, especially from accounts in risky countries, using a large number of individual and commercial accounts and directing these funds to a small number of beneficiaries.

Click here to read the full MASAK guide published in Turkish in May 2021.