GUIDANCE ON COMBATING FINANCING OF TERRORISM FOR FINANCIAL INSTITUTIONS

Ministry of Treasury and Finance
Financial Crimes Investigation Board

2025

TABLE OF CONTENTS

1. INTRODUCTION

Purpose

Although obtaining proceeds is not the primary objective of terrorists and terrorist organizations, they need financial support for their activities. Therefore, terrorist organizations try to obtain funds and transfer them to those who need it in order to conduct terrorist activities.

Terrorists and terrorist organizations use methods similar to the ones used in laundering proceeds of crime in order to hide the source of the illegally-obtained proceeds with a view to concealing the identity of the real owners of the funds used for financing the activities or avoiding the attention of the law enforcement agencies and obliged parties. Thus, it is ensured that the funds used in terrorist acts are hidden, and seizure and confiscation of the funds allocated for financing of terrorism are tried to be prevented. However, it is more difficult to trace and detect such funds compared to ML since the transactions conducted for financing of terrorism are usually in small amounts and, more importantly, since the funds may also be obtained legally.

The main characteristic that distinguishes terrorist organizations from other criminal organizations is the objective they pursue. Unlike conventional criminal organizations, the ultimate objective of terrorist organizations is not to obtain proceeds but to realize their ideologies and ensure the continuance of their activities with the proceeds they obtain. In this regard, terrorism can be financed through funds obtained from not only illegal and but also legal sources.

Although the funds obtained legally do not need to be laundered, terrorist organizations still need to hide their legal finance sources and connections. Therefore, they try to find methods similar to that of laundering in order to collect and use funds without drawing the attention of competent authorities.

Regardless of how the funds have been obtained, establishing a business relationship or conducting a transaction without paying attention to whether the funds and other assets that are the subject of the transaction are linked to terrorists and terrorist organizations will create significant reputational, operational and legal risks for the relevant financial institution. These risks are higher in cases where the terrorists or the individuals and entities associated with them have benefited from lack of supervision and monitoring procedures of the relevant institution, presence of uncontrolled areas and negligence or faulty action of the official in charge.

Therefore, in order to prevent TF abuse and avoid risks, obliged parties are required to establish and implement risk based approaches for prevention of financing of terrorism as well as measures for prevention of money laundering.

This guidance has been prepared to guide financial institutions in the prevention of financing of terrorism and it aims to set forth the risks to which the financial institutions are exposed, the measures they should take, obligations they should fulfil and the matters they should pay attention within the scope of financing of terrorism and thus to raise their awareness and increase their knowledge on this regard.

To this end, the guidance covers the offence of financing terrorism in terms of international and national regulations, sets forth the TF risk in Türkiye by including the terrorist organizations

posing a threat in Türkiye and their financing sources and methods, specifies TF-related obligations of obliged parties stipulated by Law No. 5549 and 6415 and their secondary legislation, and finally points out the matters to which financial institutions especially need to pay attention and provides case studies.

Methodology

The methodology of the Guidance on Combatting Financing of Terrorism for Financial Institutions is based on the guidance of FATF, which is the international standard setter in CFT matters and has been built on FATF guidance and recommendations with the aim of raising awareness of financial institutions and constructing a TF risk perception at national level in order to ensure the implementation of preventive TF measures.

While drawing up the guidance, technical trainings were received from experts assigned within the scope of EU AML/CFT Global Facility program and the outputs of the training were also used in the preparation of the guidance.

Terrorist financing activities involve collection, provision or use of funds. Therefore, this guidance has been drawn up to include all these activities. Besides, it is in line with the National Risk Assessment and it focuses on assessing national TF risks.

The basic concepts forming the base of the risk assessment made in this guidance can be summarized as terrorist elements posing threats and risks for Türkiye, their main financing methods and matters to which financial institutions should pay attention for combatting these elements. In line with this classification, the guidance is mainly made up of two parts: TF risk in Türkiye and matters to which financial institutions should pay attention in relation to these risks.

Fundamentally, this guidance has been prepared based on knowledge and experience of experts and managers taking part in TF analyses and evaluations in MASAK and holding consultations with the private sector during supervision of obligations. It has also benefited from the information and documents obtained from stakeholders in public and private sector and the case and typology examples in the guidance has aimed to touch different sectors and areas as much as possible.

Furthermore, the guidance has also handled the risk factors given in FATF guidance, other international documents and previous national guidance in relevant sections, made explanations specifically for areas and sectors entailing high risk and likely to be abused and provided examples of red flags.

2.TERRORISM FINANCING OFFENCE AND TF RISK IN TÜRKİYE

2.1. TF Risk in Türkiye

General Information

Financing is vitally important for terrorist organisations as it is for every individual and institution. Terrorist organisations sustain their existence as they perpetrate their acts which are only possible through financing. In other words, if terrorist organisations do not have regular financing activities or if they have deficiency of financing, "their terrorist acts and other organisational activities" will be affected/hindered. Therefore, such negative impact will lead to a loss of power and their terrorist acts will end in the course of time.

Combating the financing of terrorism is the type of combat targeting at financial activities of terrorist organisations. In Türkiye, there are several types of terrorist financing used by terrorist organisations ranging from criminal proceeds obtained through any kind of smuggling (drugs, arms, migrants, tobacco, fuel, commodities, etc.), funds collected by force or from voluntary people in places where they can penetrate (donations, aids, etc.) or by abusing of religious beliefs, to earning income via corruption or companies with legal appearance.

Terrorism has been the predominant threat against the security and stability of Türkiye for long years. Due to its geopolitical and geostrategic location, Türkiye has both been exposed to direct terrorist threat and been affected indirectly by terrorism because of being close to regions where there are intensive political instabilities and conflicts. Thus, excessive amounts of terrorism and TF threaten Türkiye.

Unlike the situation of many countries suffering from terrorism, in a difficult geographical location Türkiye, is in the position of a country that is the target of multiple large-scale terrorist organisations of internal and external origins and which are composed of multi-components, have different characters. Türkiye is simultaneously fighting these organizations that even act sometimes in coordination against itself. Financing methods of these different types of terrorist organisations with different structures change in accordance with the ideology, objective, organisational structure and size of each organisation. They obtain funds both from legal activities and usually from illegal acts, which cause Türkiye to be exposed to multidirectional TF threats.

2.2 Terrorist Organisations Threatening Türkiye, Their Financing Sources and Methods

Terrorist Organisations

Türkiye has been fighting against different forms of terrorism for years from FETO to ethnic separatist and divisive PKK, from extreme leftist terrorist organisation DHKP-C to Al-Qaida and DAESH that abuse religious beliefs.

The separatist, extreme leftist and religion-abusing terrorist organisations which threaten Türkiye's national security, territorial integrity, political union, public order, and people's and security forces' lives and properties are:

-Fetullahist Terrorist Organisation

-PKK/KCK-PYD/YPG

-Organisations abusing religious beliefs (DAESH, Al-Qaida and factions),

-Leftist terrorist organisations (DHKP-C and other leftist terrorist organisations MLKP, TKP/ML TIKKO, MKP/HKO, BÖG, MLSPB, DKP))

These terrorist organisations may also be classified as local-regional organisations (PKK, Fetullahist Terrorist Organisation, DHKP-C and other leftist organisations) and international organisations (DAESH, Al-Qaida and factions).

2.3. Financing Sources of Terrorist Organisations

Three types of financing sources can be listed. The first one is proceeds from illegal acts such as smuggling (of drugs, arms, migrants, tobacco, fuel, commodities, etc.), corruption, robbery, theft, ransom, blackmailing, racketeering, so-called tax, forgery (false ID cards, passports, etc.). The second one is proceeds from activities with legal appearance such as membership fees, donations, earnings from the sale of publications of organisations, revenues from social/cultural activities organised by legal persons like associations/foundations, etc., and also use of front companies. The third type of source is the funds obtained abroad.

The most important source of proceeds of **FETO** is "himmet" which is a kind of donation that they collect by abusing religious beliefs of the society. Although the organisation has lost much of its power within the country as a result of systematic efforts to combat it, it continues to pose a significant threat to our country, particularly through its members abroad and those within the country who have not been exposed. The organisation has focused on financing activities to motivate its members within the country. In this context, it has been observed that the organisation has recently used foreign currency transactions, money and value transfer activities, the use of crypto assets, and fundraising methods through social media platforms.

As a source of illegal proceeds, **PKK/KCK-PYD/YPG terrorist organisation** receives commissions from smugglers for any kind of smuggling acts (drugs, arms, goods, fuel, migrant, etc.) conducted especially in Türkiye; directs manufacturing and trafficking of drugs and extorts money from natural and legal persons under the guise of so-called taxation. Within the scope of legal-looking sources of proceeds, the terrorist organisation collects donations using non-profit organisations, obtains income and financial support from commercial enterprises run by its supporters, generates income from cultural-looking activities, and obtains income from product sales. The terrorist organisation also receives funding for the food, clothing, and shelter needs of terrorists in the mountains through donations or goods sales from small-scale businesses operating in the retail trade sector. In terms of external support activities, it is known that the organisation receives financial support, particularly from European countries.

It has been observed that **terrorist organisations that abuse religious beliefs** have recently been receiving financing in Türkiye through less organised methods under the name of zakat, aid, donations, etc. On the other hand, although its effectiveness has declined, DAESH continues to use social media for crowdfunding, and financing is also obtained through cryptocurrencies, money and value transfer activities, and non-face-to-face transactions.

Examination of current financing activities of **leftist terrorist organisations** (primarily DHKP/C) reveals that these organisations have a significant presence in European countries and that a large portion of their financing comes from cultural activities, product sales, donations, racketeering, and other sources in Europe. In this context, it is observed that the

organisation can secure financing through foreign currency transactions, non-face-to-face transactions, cash courier activities, and cryptocurrency transactions. In addition, it is known that these terrorist organisations also generate income from activities such as smuggling, robbery, theft, and forgery, etc. similar to the PKK/KCK-PYD/YPG.

2.3.1. Illegal Financing Sources of Terrorist Organisations

Many terrorist groups tend to perpetrate criminal acts to meet their expenses for daily operational activities, equipment, purchasing information, training, communication and travel. Terrorists increasingly carry out such acts to easily earn money.

Some of the illegal financing sources of terrorist organisations are as follows:

- **Smuggling of Drugs**

The increase in the need of financing directed terrorist organisations towards methods through which they can obtain high amounts. Thus, trafficking of drugs have become attractive and inevitable for terrorists. Besides, the greed of some members to gain personal funds is another factor that leads them to seek the ways of earning more and easier money. Terrorist organisations need financing sources that can bring them high amounts with little effort. Smuggling of drugs more than meets their needs.

Terrorist organisations obtain proceeds and finance their activities through either trafficking drugs themselves or getting commission by allowing the smugglers pass through the region they control.

- **Smuggling of Arms**

Smuggling of arms and ammunition is important for terrorist organisation for two reasons. First, terrorist organisations need them for using in their terrorist acts. Since arms and ammunition cannot be obtained legally, they have to smuggle them. Second, terrorist organisations cooperate with other criminal organisations in smuggling and they also obtain proceeds by this way.

Performing activities is essential for terrorist organisations to continue to exist, and it is only possible with arms and ammunition obtained through supports or criminal acts. Therefore, terrorist organisation have to cooperate with organised criminal organisations carrying out smuggling of arms or they have smuggle arms themselves, which depend on the conditions of the countries or regions where they carry out their acts.

- **Racketeering**

Racketeering is the act of terrorist organisations where they collect funds from businesspersons and people carrying out commercial activities under the name of “tax” by using oppression, threatening and intimidation. They can perform this act either by claiming to protect or not to harm, or by intimidating, abducting, or threatening to report a crime or a situation to authorities. In general, people who accept to give money are not members of terrorist organisations. They give money since they are afraid of the terrorist organisations and they want to protect themselves and their assets from them, which is the result of terrorist organisations’ practices of suppression and intimidation.

- **Human Smuggling**

Terrorist organisations both provide financial income and recruit personnel through human smuggling. Terrorist organizations also cooperate with human smuggling networks operating in countries other than the countries where they are located via their members in those countries, and receive a share of the proceeds of criminal networks that perpetrate human smuggling as a profession.

- **Forgery**

Terrorist organisations which can easily find all kinds of printing tools and materials and specialise in forgery due to today's developing technological opportunities both print fake passports and IDs for their members and generate income by issuing fake documents to organised crime organizations upon request.

- **Ransom and Blackmailing**

Ransom is defined as “money or salvation which one has to pay for himself or someone else in order to get rid of captivity or any kind of trouble”. In terms of terrorist organisations, it is the act of kidnapping businesspersons, well known bureaucrats, politicians, etc. and demanding money in return. Many terrorist organisations in the world are endeavouring to increase their financial sources by taking ransom especially by kidnapping businesspersons.

- **Robbery and Theft**

Robbery and theft are methods used by terrorist organisations particularly at the establishment stage to gain proceeds. Today, large business places, primarily financial institutions, set up special security systems with the help of the developing technology as a measure against such acts of terrorist organisations. In addition to security systems, ongoing development of police about their knowledge of terrorist organisations have resulted in a decline of robbery, theft and burglary acts of terrorist organisations.

2.3.2. Financing Sources With Legal Appearance

The financing of terrorist organisations is not always from illegal sources. In addition, sources with legal appearance can also be used to finance terrorist organisations. Financing of terrorism with legitimate-looking sources is expressed as "polluting clean money" or "reverse laundering".

- **Membership Fees and Donations**

The most important legal-looking funding source of terrorist organisations is the money regularly collected from the members of the organisation under the name of "membership fee" and the money provided voluntarily or under the name of "donation" from the sympathizers of the organization without any pressure, coercion or violence.

Terrorist organizations can collect donations to the front organizations and institutions they have established for different reasons, usually under the heading of humanitarian aid; or from some of their supporters directly, according to the ideology of the organization, they can request money under the name of donation or donation.

Significant amounts of money is collected through the aids provided by the sympathizers and militants of organizations. People who are not actively involved in organisational activities, but

who fully embrace the ideology of the organisation, are conscious of serving the aims of the organization with their financial contributions.

- **Abuse of Non-Profit Organisations**

It is known that NPOs are inherently vulnerable to being used for financing terrorist organisations with resources in legal appearance, and that they can be used for terrorist activities or financing of terrorism. The fact that associations and foundations have wide range of activities, credible public images, important domestic and international fund resources, operational sturdiness and geographical advantages like the opportunity to access everywhere all over the world including conflict areas make them open to be abused by terrorist organisations. In this context, methods used to abuse non-profit organisations for financing of terrorism can be observed as terrorists or terrorist organisations using non-profit organisations established through legal procedures and for legitimate purposes as a channel for financing terrorism, including by appearing as legitimate organisations to avoid asset freezing measures, and as concealing or obscuring the secret transfer of funds collected for legitimate purposes to terrorist organisations. Furthermore, the establishment of associations and foundations under the guise of legitimate purposes for the specific purpose of terrorist activities or the financing of terrorism is also among the methods of abuse.

Therefore, developing cooperation between financial institutions and non-profit organisations, preventing the misuse of non-profit organisations for terrorist purposes through preventive and repressive measures, and raising awareness on this issue among public institutions and non-profit organisations through training and awareness-raising activities, identifying the risks of the sector based on a risk-based approach, public institutions' and non-profit organisations' developing preventive measures to protect against TF abuse in accordance with their own management procedures, and transferring funds through financial institutions to remove them from cash-intensive environments are of great importance in the fight against TF.

In Türkiye, associations and foundations are registered within a system and they operate pursuant to the Law on Foundations No. 5737 and Law on Associations No.5253. They are also audited in accordance with the abovementioned laws. Besides, the Constitution, The Civil Law No 4721 and the Law on Collecting Aids No 2860 include some regulations regarding the sector. Although the numbers of associations and foundations in Türkiye are high, analyses demonstrate that the sector's TF risk is low.

- **Commercial Activities**

Terrorist organisations are also financed through legal commercial profits of entities established and run by people who used to be members of a terrorist organisation or who apparently do not have any connection with such organisations.

Some terrorist organisation try to invest their fund in commercial activities to earn proceeds. For this purpose, they establish businesses and small companies operated by people who are reliable for terrorist organisations.

- **Proceeds From Publications of the Terrorist Organisation**

In addition to using their publications like newspapers, magazines and books for spreading their ideologies and training their supporters, terrorist organisations also obtain financial resources by selling them to their sympathizers or militants.

❖ **Proceeds from Social Activities**

Terrorist organisations or their affiliated organisations provide financing by organising social activities like concerts, festivals.

2.3.3. Foreign Supports

Terrorist organisations rely majorly on foreign supports for their success. It does not seem for possible a terrorist organisation to be successful without foreign supports. Because it is very difficult to meet their needs such as food, housing, training, arms, etc. with only domestic resources. Foreign supports are transferred to terrorist organisations directly or they are used for recruiting supporters, making their propaganda or gain sympathy among the public.

2.4. Possible Methods Used by Terrorist Organisations in Their Financial Transactions

Terrorist organisations use various methods both for obtaining the financial sources they need and for making expenditures that they have to. Possible methods preferred by terrorist organisations for their financial movements can be described as follows:

- *Use of Banking System*

Financial institutions are the most important tools in the business life for domestic and international monetary movements. Terrorist and criminal organisations majorly use banks which are the fundamental actors of the financial system due to their international connections. Technological developments in payment systems, the advantages like speed and logistics increase the risk of legal financial systems to be used for terrorists' funds. Internet banking, ATMs, credit cards, pre-paid cards and travel checks which facilitate the daily life are also convenient services for being used for TF purposes.

- *Use of Alternative Remittance Systems*

As an alternative payment tool also called "underground banking", the Hawala system is a method used for transferring funds without using the traditional banking system and without any physical movement from one region to another. This trust-based, fast and cheap system is risky and very open to be abused in terms of TF due to the anonymity it ensures, the lack of requirement to give information about the source of funds and a systematic registering process.

In the Hawala system, the originator in Country A wants to send money to the beneficiary in Country B. For this purpose, the originator applies to the Hawaladar 1 in country A, and gives cash. Hawaladar 1, then, gives a Hawala code to the originator, and also to Hawaladar 2 in Country B. The originator calls the beneficiary in Country B, give him the Hawala code and the information on Hawaladar 2. The beneficiary who is in country B goes to Hawaladar 2, tells them the code and takes the cash sent to him. Hawaladars collects their commissions from the originator and/or the beneficiary in a certain rate. There is no physical fund transfer between Hawaladars at that moment, but they carry out net settlement in certain intervals. The Hawaladar who owes the other sends the amount physically with cash couriers or transfers it via legal financial system.

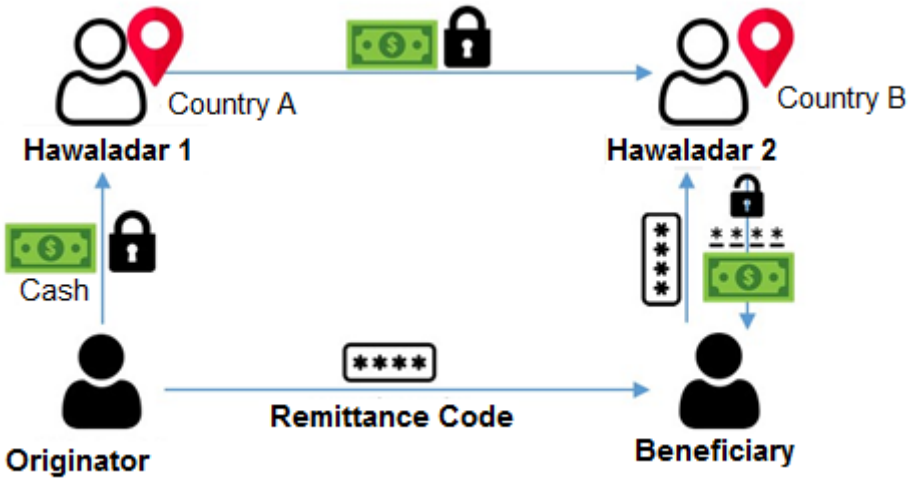

Figure 1: *Sample of Hawala Scheme*

With the development of internet banking and new financial technologies, the operating system of these networks providing irregular payment services through the so-called underground banking system has been modified. They are currently able to carry out fund transfers by operating like a payment institution by using instant messaging applications for sending passwords and codes, and by using internet banking for transferring funds to personal accounts of the Hawaladars. In addition, digital remittance applications, which can be accessed by sending a link to the mobile phones of the sender and the recipient, are also emerging as a new fund transfer mechanism within the scope of terrorism financing.

Persons operating in the Hawala system may resort to various methods to disguise their activities. It is observed that institutions such as Exchange Offices and Precious Metals, Stones and Jewellery Dealers or Intermediaries, where cash transactions may occur in high amounts and frequently, and front companies that may disguise fund transfers as commercial activities are used within the scope of remittance activities.

While Hawala systems are legal in some countries, they are illegal in others, including Türkiye. In accordance with FATF Recommendations, each country should take necessary measures for ensuring that natural and legal persons providing money or value transfer services, including transfers through informal systems or networks, are licenced and registered, and are subject to all FATF standards which banks and non-bank financial institutions are subject to. Each country should ensure that illegal providers of this service are punished with administrative, judicial and criminal sanctions.

In line with these recommendations, the abovementioned activities are punished with criminal sanctions in Türkiye.

The Law No. 6493 on Payment and Securities Settlement Systems, Payment Services and E-Money Institutions establishes in Article 28 titled “Unauthorised Operation” that officers of natural and legal persons operating like system operators, payment institutions or e-money institutions without taking authorisations required by that Law shall be punished with an imprisonment of one to three years and a judicial fine of up to five thousand days. The CBRT, which is responsible for the regulation and supervision of payment and electronic money institutions, has established a denunciation mechanism to detect unauthorised activities. A

guide on how to use this mechanism, which is accessible to all citizens via e-State, was prepared and published on the CBRT website.[1]

In general, Hawala systems do their payments and collections using legal business accounts in financial institutions. This is the moment where the financial system starts to be used and where the financial institutions can detect such illegal systems. That financial institutions submit STRs on these detections is significant since those STRs will be notified to CBRT by MASAK.

- *Use of Cash Couriers*

It is known that fund transfers carried out by terrorist organisations by using cash couriers are used for illegal purposes. Cash couriers transfer cash by carrying it in their belongings or hidden in certain compartments of their vehicles. They can both carry out domestic and international transfers. After passing through legal borders of countries, the couriers try to put the cash they carry into the financial system. In this stage, it may be possible to detect persons who carry cash in an amount that is not compatible with their profile.

- *Abuse of Commercial Activities*

Commercial enterprises and especially companies dealing with import and export can be used in order to safely deliver terrorist funds to desired destinations. While these businesses seem to be doing a real trade, in the background, the amounts that are the proceeds of this fictitious trade can be transferred to terrorist organizations, or while there is an actual commercial purpose, certain amounts hidden in this activity can be transferred to terrorist units. Thus, terrorist organizations can provide funds to themselves both in national and international commercial system by using their own or their supporters' commercial businesses. Terrorist organisations can even establish a front company and directly fund themselves. The common feature of the great majority of such companies is that high amounts of cash is deposited or transferred in their bank accounts in a short period after their establishment and then transferred to other companies.

-*Use of Payment Systems*

The risk of being used in the transfer of funds is quite high for commercial web sites and internet payment systems since the names of customers are unknown, transactions between customers are not carried out face to face, transactions can be made via different records, such websites and payment systems are accessible from all over the world, pre-payment system is accessible, pre-paid cards, gift cards or gift check can be used , and the source of funds cannot be easily traced when they are in cash.

Although Fintech and payment services provide convenience for users by being easily accessible and fast, such a convenience carries some risks together. In this scope, payment systems through mobile phones is also accepted as one of the most suitable tools for receiving and transferring funds by criminals and terrorists.

-*Use of Social Media Platforms*

[1] Application Guide for Reporting Individuals and Organizations Providing Unauthorized Payment Services to the Central Bank of the Republic of Türkiye (TCMB, 2022)

Social media platforms can also be abused for TF purposes. Funds are collected by crowdfunding method either by sharing IBAN or wallet information on these platforms or by using the features of "donation" or "gift" through TikTok, Twitch, Youtube, etc.

- *Use of Crypto Assets and CASPs*

The developing technology has led to the spread of crypto currencies which are also used by terrorists. Crypto currencies are not controlled by authorities or governments, and they can be easily transferred to and from individuals' wallets. The fact that it is very difficult to determine the identity of electronic wallet holders is another risk factor in terms of TF. Therefore, CASPs are vulnerable to be abused for TF purposes.

It has been recently observed that terrorist organisations try to collect funds through anonymous coins known to be privacy-based, and some groups working for terrorist organisations on Internet-based texting applications direct people to using these coins for transferring "donations".

2.5. TERRORISM FINANCING CRIME

2.5.1. Terrorism Financing Crime in International Regulations

The UN International Convention for the Suppression of the Financing of Terrorism of 1999 defines the purpose of terrorism as o intimidate a population, or to compel a government or an international organisation to do or to abstain from doing any act. The Annexes of This Convention are nine conventions and protocols that were prepared by UN since 1970 for fighting against terrorism related to the security of air and maritime transportation activities, the security of Diplomatic activities and the protection of mass destruction weapons.

The essential property of the convention is that it defines terrorism financing as an individual crime and that it establishes the seizure of proceeds used or to be used for TF or to be obtained through TF. Article 2 of the Convention explains the financing of terrorism. According to the Article, if a person provides or collects funds with the intention that they should be used or in the knowledge that they are to be used, in full or in part, for the acts specified in the Convention, this is called terrorism financing. The Convention not only defines terrorism financing as a crime, it also establishes some practicable measures to prevent this crime. Part of these measures are for ensuring international assistance while the other part are for the suppression of sources financing terrorism. The Convention requires for detecting and seizing funds used or prepared to be used for TF that the States which are parties to that Convention introduce some obligations for banks, fund transferring institutions and other financial institutions such as customer identification, not opening an account without the name of the customer, reporting suspicious transactions, etc., and for monitoring cross-border cash movements as it is in the case of FATF's 40 Recommendations+11 effectiveness criteria.

The EU Directive 2015/849 "On The Prevention Of The Use Of The Financial System For The Purposes Of Money Laundering Or Terrorist Financing", prepared against TF specifies in Article 1 that member countries shall ensure that money laundering and terrorism financing are prohibited. Article 1 of the Directive 2017/541 states that member countries shall ensure that intentional acts which can seriously cause harm to a country or an international organisation due to their nature and context and which are defined as crimes according to their domestic

legislation are defined as terrorism crimes where they occur. Article 11 of the same Directive defines the TF crime.

The EU Directive 2015/849 defines beneficial owner and politically exposed persons, prohibits opening nameless accounts, explains how to carry out non-face-to-face transactions and correspondent banking transactions, and detailed regulations are set forth regarding CDD. The Directive 2019/1153 emphasizes that obliged parties should pay special attention to extraordinary, complicated, large-scale transactions without any economic and legal purpose due to the possibility that they may be connected with ML and TF. This Directive also specifies that if there is any information, suspicion or grounds to suspect that ML or TF offence was committed, obliged parties should report the case to FIUs.

In addition to the convention on TF, under the UN Charter Chapter VII, UN also establishes binding measures regarding the implementation of targeted financial sanctions for CFT. Compliance with measures is also dealt with by FATF's Rec. 6 and Effectiveness Criteria 10. Within this framework, two essential sanction regimes stand out:

- 1267(1999), 1988(2011), 1989(2011), 2253(2015) Al-Qaida, DAESH, Taleban
- 1373 (2001) Other Terrorist Organisations

Other significant UNSC Resolutions are:

- 1452 (2002) Getting Authorisation from Sanctions Committee for accessing frozen funds
- 1730 (2006) Assigning UNSC Focal Point for objections to sanctions
- 1904 (2009) Establishment of Ombudsman in UNSC for objections to sanctions
- 2270 (2014), 2178 (2014) Prevention of financing FTFs for travelling and training purposes

2.5.2 Terrorism Financing Crime in Turkish Legislation

The Anti-Terror Law No. 3713 defines terrorism as "any kind of act attempted by one or more persons belonging to an organization with the aim of changing the characteristics of the Republic as specified in the Constitution, its political, legal, social, secular and economic system, damaging the indivisible unity of the State with its territory and nation, endangering the existence of the Turkish State and Republic, weakening or destroying or seizing the authority of the State, eliminating fundamental rights and freedoms, or damaging the internal and external security of the State, public order or general health by using pressure, force and violence with one of the methods such as terror, intimidation, oppression or threat."

According to Article 4(1) of the Law No. 6415, any person who provides or collects funds for a terrorist or terrorist organisations with the intention that they are used or knowing and willing that they are to be used, even without being linked to a specific act, in full or in part, in perpetration of the acts that are set forth as crime within the scope of Article 3 shall be punished by imprisonment for a term of five to ten years, provided that his/her act does not constitute another offence requiring a heavier punishment.

Acts for whose perpetration collecting or providing funds are forbidden are as follows pursuant to Article 3 of the Law No. 6415:

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

3. FINANCIAL INSTITUTIONS AND THEIR OBLIGATIONS WITHIN THE SCOPE OF TERRORISM FINANCING

3.1. Obligations of Financial Institutions Within the Scope of Law No 5549 On Prevention Of Laundering Proceeds Of Crime And Related Legislation

Relevant legislation has identified "obliged parties" and described "obligations" within the scope of preventive measures in order to prevent ML and TF, ensure effectiveness against these crimes and hinder the abuse of financial system by criminals.

3.1.1. Obliged Parties

Financial institutions defined as obliged parties, designated non-financial businesses and professions (DNFBPs) and other obliged persons are at risk of being used as an intermediary by criminals for illegal activities such as financing terrorism due to the nature of their activities and the scope of the services they provide. In other words, financial transactions or services provided by obliged persons may be abused by malicious persons by being used in the execution of criminal acts. In order to prevent it and to raise the awareness of the obliged parties on ML and TF offences and the fight against these offences, it has been tried to ensure that they undertake a 'preventive' function. Therefore, obliged persons are the most important stakeholders of MASAK in the fight against crime.

The obliged parties are defined in subparagraph (d) of the first paragraph of Article 2 of the Law No. 5549 on Prevention of Laundering Proceeds of Crime and the first paragraph of Article 4 of the Regulation on Measures (RoM). In Article 2(1)(d) of the Law, the obliged parties in terms of their fields of activity are those operating in the fields of banking, insurance, private pension, capital markets, money lending and other financial services, post and transport, games of chance and betting; those who are engaged in the trade of foreign currency, real estate, precious stones and metal, jewellery, transport vehicles, business machines, historical artefacts, works of art and antiques or those who act as intermediaries in these activities, notaries, sports clubs, lawyers limited to the activities specified in the law and those who operate in other fields determined by the President. Obliged parties are is listed one by one in the Regulation on Measures.

In of Article 3(1)(f) of RoM, the obliged parties listed in subparagraphs (a) to (h), (m) and (ü) of the first paragraph of Article 4 of RoM and Post and Telgraph Organization (PTT Corporate/The Turkish Post) limited to banking activities are defined as 'financial institutions'. And the obliged parties listed in subparagraph (m) of the first paragraph of Article 3 and subparagraphs (k), (n), (s), (s), (ş), (t) and (u) of the first paragraph of Article 4 of RoM are defined as DNFBPs. Other obliged parties are obliged parties that are not included in these two groups. In this context, financial institutions are:

a)Banks.
b) Institutions other than banks who have the authority to issue bank cards or credit cards
c)Authorized exchange offices given in legislation on foreign exchange
ç) Financing and factoring companies
d) Capital Markets Brokerage Houses and portfolio management companies
e) Payment service providers and electronic money institutions
f) Investment partnerships

g) Insurance, reinsurance and pension companies, and insurance and reinsurance brokers.
ğ) Financial leasing companies
h) Institutions furnishing settlement and custody services within the framework of capital markets legislation
i) PTT Corporate (Company of Post and Telegraph Organisation)
m) Precious metals intermediaries
ü) Crypto Asset Service Providers (CASPs)

3.1.2. Obligations

The obligations of obliged parties are specified in Articles 3 to 9/A of Law No. 5549 and details of these obligations are given in secondary legislation.

The obligations of FIs under Law No. 5549 are as follow:

- Customer Due Diligence

According to Article 3 of Law No. 5549, the obliged parties are required, within the scope of the principles regarding customer due diligence, to identify the persons carrying out transactions and the persons on behalf or for the benefit of whom the transactions are conducted within or through the obliged parties before the transactions are conducted, and to take other necessary measures.

The details of customer due diligence are regulated in Articles 5 to 26/A of RoM. The essential measure required to be taken within the scope of customer due diligence is "customer identification". The Regulation elaborates how and in which transactions customers will be identified and classifies the transactions requiring customer identification by specifying if a threshold will apply or not.

According to the Regulation, obliged parties are required to identify their customers and verify their identification information;

- Regardless of the monetary amount when establishing permanent business relationships;
- Regardless of the monetary amount in cases requiring STR;
- Regardless of the monetary amounts in cases where there is suspicion about the adequacy and the accuracy of previously acquired identification information.

Besides, obliged parties are also required to identify their customers and take necessary measures to determine the beneficial owner of the transaction:

- When the amount of a single transaction or the total amount of multiple linked transactions is equal to or more than 185.000 TL (for CASPs 15.000 TL);
- When the amount of a single transaction or the total amount of multiple linked transactions is equal to or more than 15.000 TL in wire transfers and crypto asset transfers carried out by CASPs.

The customer identification should be complete before the business relationship is established or the transaction is conducted.

Article 22 of RoM regulates rejection of transaction and termination of business relationship. The Article stipulates that business relationship will not be established and transaction will not be conducted in cases where customers cannot be identified or adequate information on the

purpose of the business relationship cannot be obtained. Furthermore, the business relationship is required to be terminated and the case should be evaluated to determine if such issues are suspicious in cases where customer identification and its verification which are required to be conducted in case of suspicion on the adequacy and accuracy of previously obtained customer identification information cannot be carried out.

Article 2/A of RoM establishes the originator and recipient information that should be given in crypto asset transfers, and relevant measures that should be taken.

MASAK General Communiqué No.29 (published in the Official Gazette No. 32940 on June 28, 2025) prepared based on Article 26/A of RoM and Article 13 of RoC (Regulation on Compliance) regulates enhanced measures to be applied by crypto asset service providers in their relationships with their customers.

- Customer Due Diligence for the Beneficial Owner

Beneficial owner is defined in Article 3(h) of RoM as "*natural person(s) who has ultimate control or influence over natural persons conducting transaction within an obliged party, or over natural persons, legal persons or unincorporated organizations on whose behalf a transaction is being conducted within an obliged party*".

Article 17/A of the same Regulation explains how to identify the beneficial owner:

- Obliged parties shall take necessary measures in order to identify the beneficial owner.
- When establishing permanent business relationship with legal persons registered to trade registry, obliged parties shall identify, in accordance with article 6, the natural person partners holding more than 25% of the legal person's shares as the beneficial owner.
- In cases where there is a suspicion that the natural person partner holding more than 25% of the legal person's shares is not the beneficial owner or where there is no natural person holding a share at this rate, necessary measures shall be taken in order to identify the natural person(s) who is/are ultimately controlling the legal person. Natural person(s) identified shall be considered as beneficial owner.
- In cases where the beneficial owner is not yet identified, the natural person(s) holding the position of senior managing official in the trade registry with the highest executive authority, shall be considered as beneficial owner.
- Within the scope of permanent business relationship, , necessary measures shall be taken in order to identify the natural person(s) who is/are ultimately controlling other legal persons and unincorporated organizations. In case where the beneficial owner is not identified, the natural person(s) holding the position of senior managing official with the highest executive authority within them shall be considered as beneficial owner.
- Obliged parties shall identify the beneficial owner and take necessary measures in order to verify the beneficial owner. In this framework, a notarized circular of signature including identity information can be used.
- When establishing permanent business relationship with legal persons registered to trade registry, obliged parties shall also identify, in accordance with article 7, the legal person partners holding more than twenty-five percent of the legal person shares. Identity information required to be taken from non-resident legal person partners may be verified through open sources of the institutions in relevant country which are counterparts of the Union of Chambers and Commodity Exchanges of Türkiye or other institutions which keep data officially.

Identification of beneficial owner is significant for combating the financing of terrorism as well as for compliance with the obligation of the implementation of asset freezing decisions given due to TF reasons.

Guidances published by MASAK, the Frequently Asked Questions page on MASAK web site and FATF Guidelines may be used for compliance this obligation.

Besides, the beneficial owner registry made by the Revenues Administration pursuant to the General Communiqué No. 529 on Tax Procedure Law (Published on the of No. 31540 on 13th July 2021) is another tool that can serve for obliged parties to comply with this obligation. According to the Communiqué, corporate tax payers must report their beneficial owners to the Revenue Administration four times a year along with their provisional and annual tax returns, while other taxpayers must report them once a year. Any changes in beneficial owners must also be reported within one month. Although the relevant registry is not publicly accessible due to tax confidentiality, the Revenue Administration has provided indirect access to the information in the registry due to the importance of the matter. Accordingly, taxpayers can log in to the Digital Tax Office and obtain a QR code-enabled document showing their beneficial ownership status as declared in the registry. Obliged parties can also verify this document, which they will request from their customers, using the QR code on it. Thus, obligated parties will be able to compare the beneficial owner information they have identified in accordance with their obligations under RoM with the registration information declared by the customer to the Revenue Administration. In the event of a discrepancy between the two pieces of information, a suspicious transaction report should be submitted to the Revenue Administration.

- Periodical Reporting

According to Article 6 of Law No. 5549, obliged parties are required to report the transactions, to which they are parties or intermediaries, exceeding the amount determined by the Ministry to MASAK. The transaction types subject to periodical reporting, reporting procedures and periods, excluded obliged parties and other implementation principles and procedures are determined by MASAK.

- Providing information and documents

According to Article 7 of Law No. 5549, when requested by MASAK or by examiners, the public institutions and organizations, natural and legal persons, and unincorporated organizations are required to fully and accurately provide all kinds of information, documents and related records in every type of environment, any kind of information and passwords necessary for accessing to or making these records decipherable, and render necessary convenience.

Those from whom information and documents are requested in accordance with the previous paragraph cannot avoid giving information and documents by alleging the provisions of special laws, provided that the defence right is reserved.

- Retaining and submitting

According to Article 8 of Law No. 5549, obliged parties are required to retain the documents, books and records, identification documents kept in all forms regarding their transactions and obligations established in this Law for eight years starting from the drawn up date, the last record date, the last transaction date respectively and submit them when requested.

- ***Electronic notification***

According to Article 9/A of Law No. 5549, the notifications to be made by FIs listed in Article 7(1) of Regulation on Principles and Procedures for Electronic Notification System (banks, capital market intermediary institutions, financial leasing companies, finance companies, insurance and pension companies, portfolio management companies, Central Securities Depository, PTT Corporate and CASPs) within the scope of implementation of Law No. 5549 and the Law No.6415 on Prevention of the Financing of Terrorism are required to be notified and responded electronically notwithstanding the procedures relating to electronic notification established in Article 7/A of Notification Law No.7201.

- ***Establishing a Compliance Program and Exclusive Assignment of Compliance Officer***

According to Article 5 of Law No. 5549, Ministry has the authority to determine obliged parties and implementation principles and procedures within the scope of necessary measures including assigning an officer with necessary authority at administrative level for ensuring compliance with this Law at obliged party and financial group level and establishing training, internal control and control and risk management systems with a risk-based approach.

The principles and procedures for establishment of compliance programs by obliged parties are regulated in Regulation on Program of Compliance (RoC) introduced pursuant to Article 5 of Law No. 5549.

The obliged parties that are required to establish a compliance program are listed in Article 4 of RoC.

According to Article, the obliged parties that are required to establish a compliance program are:

a) Banks (Except for Central Bank of Republic of Türkiye, Istanbul Settlement and Custody Bank),

b) Capital Markets Brokerage Houses

c) Insurance and pension companies

ç) Postal and Telegraph Corporation (pertaining only to banking activities)

d) Group A authorised exchange offices listed in the foreign exchange legislation

e) Financing, factoring and financial leasing companies,

f) Portfolio management companies,

g) Precious Metals brokerage houses,

ğ) Electronic money institutions

h) Payment institutions (excluding those providing exclusively brokering services for payment of bills, those providing exclusively payment order starting services, and those providing exclusively services of presenting information of payment account),

ı) Crypto Asset Service Providers.

Article 5 of RoC stipulates that the compliance program to be established on risk based approach for the purpose of ensuring the required compliance with the Law and secondary legislation issued in accordance with the Law shall include the following measures in order to prevent laundering proceeds of crime and financing of terrorism:

* institutional policy and procedures,
* risk management activities,
* monitoring and controlling activities,
* compliance officer and the compliance unit,

* training activities,
* internal audit activities.

Besides, obliged parties who will exclusively assign a compliance officer are specified in Article 29 of RoC. According to Article, the Central Bank of Republic of Türkiye, Istanbul Settlement and Custody Bank, institutions other than banks who have the authority to issue bank cards or credit cards, group B authorized exchange offices given in legislation on foreign exchange, reinsurance companies asset management companies, payment institutions (those providing exclusively brokering services for payment of bills, those providing exclusively payment order starting services, and those providing exclusively services of presenting information of payment account), cargo companies and institutions furnishing settlement and custody services within the framework of capital markets legislation, medium, large or very large scale electronic commerce service providers, agents conducting all gambling and betting activities exclusively in an electronic environment without a physical place of business and without face-to-face contact with the customer, in accordance with the relevant legislation, and savings finance companies, are obliged to assign compliance officer at administrative level within 30 days following obtaining an operating license without establishing a compliance program mentioned in this Regulation.

In accordance with the amendment published in the Official Gazette No. 32763 of 25 December 2024, institutional policies shall include efforts to identify, assess, monitor and mitigate the risks of violation, failure to implement and abstention from implementing asset freezing decisions taken in accordance with the Law No. 6415 on Prevention of the Financing of Terrorism of 7 February 2013 and the Law on No. 7262 on Prevention of the Financing of the Proliferation of Weapons of Mass Destruction of 27 December 2020. Furthermore, within the scope of monitoring and control activities under institutional policies, measures should be taken to continuously monitor customers and transactions, taking into account the decisions to freeze assets and potential matching criteria. In this context, the originator and recipient information contained in electronic transfer and crypto asset transfer messages should also be taken into account.

During their risk management, monitoring, and control activities, compliance officers appointed exclusively for that position shall also carry out enhanced controls to ensure the implementation of sanctions and to address risks related to the violation, failure to implement, or abstention from implementing asset freezing decisions under Law No. 6415 and Law No. 7262. In this context, measures should be taken to continuously monitor customers and transactions, taking into account asset freezing decisions and potential matching criteria.

The amendment published in the Official Gazette No. 32763 of 25 December requires entities that are not obligated to establish a compliance programme or exclusively appoint a compliance officer to implement risk management, monitoring, and control activities to prevent violations of asset freezing decisions under Law No. 6415 and Law No. 7262, failure to implement them, and avoidance of them, as well as to implement advanced controls for the application of the aforementioned sanctions. In this context, they are responsible for taking measures to continuously monitor customers and transactions, taking into account asset freezing decisions and potential matching criteria.

- Suspicious Transaction Reporting (STRs)

STRs are among the most important elements of AML/CFT. They aim to detect and prevent ML/TF activities through cooperation between obliged parties and the financial intelligence unit (MASAK). Suspicious transaction is defined in Article 27 (1) of RoM. The principles

and procedures for suspicious transaction reporting are regulated in Article 27 to 30 of RoM and General Communique of the Financial Crimes Investigation Board (No. 13).

Suspicious transaction is the case where there is any information, suspicion or reasonable grounds to suspect that the asset, which is subject to the transactions carried out or attempted to be carried out within or through the obliged parties, has been acquired through illegal ways or used for illegal purposes and is used, in this scope, for terrorist activities or by terrorist organizations, terrorists or those who finance terrorism

"*Suspicion"* is a subjective condition arising in people conducting and/or intermediating a transaction, thinking that the fund or the assets which is the subject of the transaction may have been derived from illegal sources or may be used for illegal purposes. The obliged party evaluates the case subjectively and makes a judgment by taking into account his/her perception and insight, the customer's behaviour during the transaction, previously obtained information on the customer, compatibility between the transaction amount and financial profile customer and other elements.

In case of suspicious transactions, obliged parties should make inquiries about the transaction within the limits of their authority and capabilities, and report the suspicion transaction to MASAK by filling out an STR form based on the available information and findings, immediately in cases where delay would be detrimental, and within 10 working days from the date of suspicion in other cases.

Suspicious transactions are reported to MASAK without seeking any monetary threshold. STRs reported within the scope of periodical reporting do not cancel the obligation of suspicious transaction reporting.

The term transaction in "suspicious transaction" is not limited to only one transaction and may include more. A single STR form is filled out for transactions that raise suspicion when evaluated together.

Besides, obliged parties cannot disclose to anybody including the parties of the transaction that they reported a suspicious transaction except the examiners assigned to conduct supervision of obligations and the courts during legal proceedings. In the event of a breach of this obligation, the person committing the breach shall be punished with imprisonment for a term of one to three years and a judicial fine of up to five thousand days, in accordance with Article 14 of Law No. 5549 entitled 'Criminal penalties for breach of obligations'.

- Suspension of Transactions

According to Article 19/A of the Law No. 5549, In cases where the assets which are the subject of a transaction are suspected to be linked to offence of laundering or financing of terrorism, the Minister shall be authorized to suspend the transactions that are attempted to be conducted or currently going on within or through obliged parties for seven work days or not to allow the performance of those transactions for the same period of time so that MASAK can verify the suspicion, analyse the transaction and convey the results of those analyses to competent authorities when necessary.

In the event that there is document or serious indication supporting the suspicion terrorist financing offence, obliged parties shall submit an STR to MASAK including relevant justifications and the request for postponing the transaction. **The transaction about which an STR with postponement request is submitted must have the indications such as being extraordinary, having subject(s) related or possibly related with crime according to the results of research done through various data bases** or other sources, or the completion of

the transaction posing **a risk that may prevent or make difficult the seizing of funds possibly related with financing of terrorism or proceeds of crime**. Obliged parties shall abstain from carrying out the transaction until MASAK notifies them the Minister's decision about the transaction. Duration of the postponement may not exceed seven working days following the date on which the STR is submitted.

3.1.3 Supervision of Obligations

Obliged parties' compliance with obligations are supervised through supervision of obligations and administrative and judicial sanctions are imposed on those who violate obligations.

"Supervision of obligations" regulated in Article 11 of Law No. 5549 is divided into two groups as "supervision of compliance with obligations" that is conducted for determining obliged parties' compliance with obligations and "examination of violation of obligations" conducted for determining violations of obligations. These are regulated in detail in RoM Chapter Six, titled "Supervision of Obligations".

"Supervision of compliance with obligations" is basically a conformity audit. It is conducted to determine if obliged party activities comply with the legislation, the measures taken are adequate and the practices are effective. The supervision can be carried out either on a standalone basis or as part of a specific supervision program. Examination of violation of obligations, on the other hand, is an audit conducted for detecting any violation of obligation and for finding out the type, number, and date of the violation and the persons responsible in case of any violation.

Obligations are supervised through examiners listed in Article 2 of 5549. These examiners are Treasury and Finance Experts employed at MASAK, Tax Inspectors, Customs and Trade Inspectors, Sworn-in Bank Auditors, Treasury Comptrollers, Insurance Supervisory Experts and Actuaries, Banking Regulation and Supervision Agency and Capital Markets Board Experts and Central Bank Auditors and Experts.

The examiners assigned to conduct supervision are authorized to request all kinds of information, documents and legal books from natural and legal persons including the public institutions and organizations, and unincorporated organizations, to examine all kinds of documents and records within them and to receive information from the relevant authorities verbally or in writing. They also use the powers given to them by other laws.

Examiners are also required to report violations of obligations to MASAK if they detect any while fulfilling their own duties entrusted to them by their units.

The reports prepared and conveyed to MASAK by examiners based on the supervision of obligation are evaluated in terms of compliance with reporting standards and whether there is any material or legal mistake. Necessary action is taken based on evaluations made. Administrative fines are imposed depending on the nature of violations or the case is referred to Public Prosecutor's Office.

3.1.4 Sanctions for Violating Obligations

The administrative fines applying to violations of the obligations of customer due diligence, periodical reporting and suspicious transaction reporting under Article 13 (1) of Law No.5549 are imposed separately on each violation by being increased in accordance with revaluation

rates. **If the obliged party is an FI**, the administrative fine is applied **twofold, not to be less than five percent of the transaction amount.**

On the other hand, according to Article 13 (2) and (3) of Law No. 5549, in case of determining that the obligations in the Article 5(1) of the Law are violated, a written warning and a period is given to obliged parties. In cases where the deficiencies are not addressed at the end of this period, the administrative fine specified in the law is imposed by MASAK by being increased in accordance with the revaluation rate; and the obliged party is given a second warning and a new period. If the deficiencies are not addressed at the end of this period, an additional administrative fine that is twice the first administrative fine is applied. If the deficiencies are not addressed within thirty days from the notification of the second administrative fine, the situation is notified to the relevant institution in order to suspend or restrict the activities of the obliged party for a certain period of time or to take measures for the cancellation of the activity license. Besides, the member of the board of directors or else the senior manager in charge, who do not comply with the obligations is given the one fourth of the administrative fine imposed on the obliged party.

Besides, the obliged parties who conduct the transaction that has been suspended or has not been allowed to be conducted pursuant to Article 19/A of the Law shall be punished by MASAK with an administrative fine in the amount of the transaction. However, the administrative fine to be imposed cannot be less than fifty thousand Turkish Liras.

In this scope, the administrative fines for each violation and their upper limits to be imposed under Article 13 of Law No. 5549 in 2025 are given in the table below.

Table 1: Administrative Fines for 2025

Obligation	Administrative Fine for Single Violation (TL)	Upper Limit of the Administrative Fine (TL)
Customer Due Diligence (5549 Art. 3)	453.342 not to be less than five percent of the transaction amount	302.232.487
Periodical Reporting (5549 Art. 6)	453.342 not to be less than five percent of the transaction amount	302.232.487
Suspicious Transaction Reporting (5549 Art. 4(1))	755.566 not to be less than five percent of the transaction amount	302.232.487
Training, internal audit, control and risk management systems, and other measures (5549 Art 5)	first warning and period 3.777.903 if the deficiency has not been addressed by the end of the period second warning and period 7.555.806 if the deficiency has not been addressed by the end of the period	302.232.487
Electronic Notification (5549 Art. 9/A)	302.229	7.555.808

Additionally, those who fail to comply with the obligations of 'providing information and documents', 'retaining and submitting' and confidentiality of suspicious transactions reports shall be sentenced to imprisonment from one year to three years and to judicial fine up to five thousand days, as stipulated by Article 14(1) of Law No. 5549

3.2 Obligations of Financial Institutions within the Scope of Law No 6415 on the Prevention of the Financing of Terrorism and Related Legislation

For the purpose of ensuring an effective fight against terrorism and financing of terrorism, Law No. 6415 on Prevention of Financing of Terrorism was put into force on 16 February with the aim of setting the principles and procedures for the implementation of the "International Convention for the Suppression of Financing of Terrorism" dated 1999 and the United Nations Security Council Resolutions related to combating terrorism and the financing of terrorism within the context of the Law, establishment of financing of terrorism offence, and freezing of assets for prevention of financing of terrorism. Additionally, for the implementation of Law No.6415, Regulation on the Procedures and Principles Regarding the Implementation of Law on the Prevention of the Financing of Terrorism (RoTF) was put into force by being published in the Official Gazette No 28663 of 31 May 2013 with a view to regulate principles and procedures for making, executing, revoking of the asset freezing decisions, and management and control of frozen assets within the scope of effective fight against terrorism and financing of terrorism.

In this scope, Law No 6415 introduced an asset-freezing mechanism as a preventive measure for combatting TF.

Asset, funds and freezing of asset are defined as follow in Law No. 6415 and RoTF.

Asset is defined in 6415 as funds, proceeds, and benefits and values derived from them or inter-conversion of them, owned or possessed or directly or indirectly controlled by a natural or legal person, and it is defined in RoTF as the fund, all kinds of proceeds jointly or wholly owned or possessed or directly or indirectly controlled by a natural or legal person, and the benefits and values gained from them or generated from conversion of them into one another.

Fund is defined in 6415 as money or property, right, claims of every kind whether movable or immovable, tangible or intangible which could be represented by money and all kinds of documents representing them, and it is defined in RoTF as money or any instruments such as bank credits, bank or travellers cheque, money orders, securities, shares, guarantees, bill of exchange, bonds, policies, letter of credits and property, right, claims of every kind whether movable or immovable, tangible or intangible, however acquired, which could be represented by money and all kinds of documents in any form, including electronic or digital, evidencing title to, or interest in such assets.

Freezing of asset is defined in Law No. 6415 as removal or restriction of the power of disposition over the asset for the purpose of preventing obliteration, consumption, conversion, transfer, assignation, conveyance and other dispositional actions of the asset, and it is defined in RoTF as removal of the power of disposition over the asset for the purpose of preventing obliteration, consumption, conversion, transfer, assignation, conveyance and other dispositional acts of the asset or restriction of it within the framework of transactions permitted to be carried out in the second and third paragraphs of Article 13 of the Law.

Article 5 of the Law stipulates decisions on freezing of assets under the possession of persons, institutions and organizations designated through the United Nations Security Council Resolutions 1267(1999), 1988 (2011), 1989 (2011) and 2253 (2015) are executed without delay through the decision of the President published in the Official Gazette.

Besides, Article 6 of the Law stipulates that in case of a request made by the government of a foreign country to Türkiye on freezing of asset under the possession of a person, institution or organization, the request will be assessed by the Assessment Commission and the decision on the request will be made by the President.

In addition, Article 7 of the Law sets forth that apart from the subjects regulated in Articles 5 and 6, following the definitive judgement of the court about the terrorist organization and based on reasonable grounds the person, institution or organizations have committed the acts within the scope of Article 3 and 4, the Minister of Interior and Minister of Treasury and Finance may jointly decide upon the suggestion of the Assessment Commission to freeze their assets in Türkiye or to repeal the freezing decision regarding their assets in Türkiye if reasonable grounds cease.

Freezing of Assets under the possession of persons and entities listed pursuant to Article 5, 6 and 7 of Law No. 6415

Article 11 of Law No. 6415 stipulates that the decisions on freezing and unfreezing of asset made in accordance with the provisions of the Law will be published in the Official Gazette, and they will be accepted as notified on the date of their publication in the Official Gazette, to the relevant person or institution about whom the decision on freezing of asset has been made.

Besides, the freezing decision will be notified to relevant public institutions, banks and other FIs by MASAK following its publication in the Official Gazette. As it is stipulated by Article 12 (4) and (5) of Law No. 6415 and Article 14 (1) and (2) of RoTF, asset-freezing decisions is required to be implemented without delay in accordance with the procedure given in Article 128 (3) to (7) of Criminal Procedure Law No. 5271, and natural and legal persons, and public institutions **that have been requested to carry out the asset-freezing decision** are required to take necessary actions and provide MASAK with information about the frozen assets **within seven days as of the date of request (notification)** in cases where they **keep** assets records of the designee.

Article 13 (1) of 6415 sets forth that management of the asset decided to be frozen are under the responsibility of the relevant natural or legal person; however, except the operations listed in the Article 13(2) and (3), **the persons whose asset has been frozen are prohibited from carrying out actions for obliteration, consumption, conversion, transfer, assignment, conveyance and other dispositional actions of the asset, and natural and legal persons, public institutions or organizations requested to execute the decision on freezing of asset are also not allowed to perform or facilitate such actions**. Paragraph (2) of the same Article states that certain actions may be carried out under the permission of MASAK for the purpose of ensuring the subsistence of the person about whom a decision on freezing of asset has been made and of the relatives of whom he/she is obliged to take care, or continuance of operations of the business enterprises or other legal persons about whom a decision on freezing of asset has been made. In addition, matters relating to the management of frozen assets are regulated in detail in MASAK General Communiqué No: 12 in accordance with the procedures and principles set forth in the Law and Regulations on this subject.

The penal provisions are regulated in Article 15 of Law No. 6415. The Article stipulates that persons who do not obey or who neglect or delay to obey the decision made regarding freezing of assets in accordance with this Law shall be punished by an imprisonment for a term of six

months to two years or a judicial fine unless such act constitutes a serious offence requiring a heavier penalty. Persons who willingly provide or collect funds or provide financial services, knowing their natures, for the benefit of individuals, entities and organisations about whom decision of freezing of assets has been made pursuant to articles 5 to 7 of this Law, or for entities controlled directly or indirectly by them, or for individuals or entities who act on their behalf or for their benefit shall be punished with an imprisonment of one to three years or a judicial fine unless such act constitutes a serious offence requiring a heavier penalty. In case that the person who does not obey the decision on freezing of assets made within the context of paragraph (1), or who provides or collects funds or provides financial services within the context of Paragraph (2) of Article 15 of Law No 6415 is an organ or a representative of a legal person; or a person, who is not the organ or representative but undertakes a duty within the scope of that legal person's operational framework, this legal person shall be punished with an administrative fine from 10,000 up to 2.000.000 Turkish Liras. However, the administrative fine cannot be less than the amount of the transaction if it is detected.

MASAK has published a guidance[2] on its website for obliged parties in order to eliminate potential uncertainties regarding whether natural and legal persons, as well as public institutions that maintain records of assets, are acting in accordance with asset freezing decisions; and to ensure that the management of frozen assets is carried out in compliance with the provisions of the Law, and that such freezing decisions are implemented fully and effectively.

4. ISSUES FINANCIAL INSTITUTIONS SHOULD PAY SPECIAL ATTENTION IN COMBATTING TERRORISM FINANCING AND CASE STUDIES

4.1 General Indicators and Suspicious Transaction Types on Risks Included in National and International Legislation

4.1.1 Risk Classification

The financial or reputational loss possible to be confronted by obliged parties of their employees due to reasons such as being abused for TF purposes or partial compliance with laws and regulations and communiqués based on laws is the risk of activities to be carried out incompliant with TF legislation.

Fundamental objective of risk management within this framework is to ensure defining, rating, assessing and mitigating possible TF risks. Implementing the parameters properly and designing relevant processes correctly ensure that financial institutions manage potential risks by monitoring and controlling their customers.

In FATF guidelines and national legislation, TF risks of financial institutions are classified in three categories which are "Customer Risk", "Service Risk" and "Country Risk".

- Customer Risk

[2] Guidance for Freezing/Unfreezing of Assets (MASAK, 2022)

Customer risk means risks possible to be confronted by financial institutions due to the fact that customers' activity fields facilitate intensive cash use, trading high-value goods or international fund transfers, or customers or persons acting for the benefit of the customers have TF purposes.

Identifying potential TF risks of customers is quite important for drawing up the general risk profile. Financial institutions determine risk scores depending on certain scales as a result of assessments made accordingly. These risk scores will be used as parameters in recruiting customers and determining customer monitoring and controlling activities. General examples of parameters used for risk scoring are demographic information, occupation, commercial activities, nationality, region of residence, financial profile, etc.

- Service Risk

Service risk means possible risks to be confronted due to non-face-to-face transactions, private banking, correspondent banking or new products to be provided using new technologies such as e-money, crypto currencies etc.

New products and services require to be assessed with risk-based approach before being launched regarding the possibility to be used for TF. Compliance units should be involved in such assessments. The effects of these services and products should be monitored with risk-based approach after they are launched.

- Country Risk

Country risk means possible risks to be confronted by financial institutions when establishing business relationships and carrying out transactions with citizens, companies and financial institutions of countries that do not have sufficient CFT legislation, do not adequately cooperated for combating such crimes or are assessed to be risky by competent international organisations.

There is not an agreed definition of regions requiring to be classified as high-risky. Transactions of customers who have connections with countries that are assessed to have inadequate legislation or monitoring, control and tracking processes against TF should be carried out with risk-based approach, and they should be monitored and controlled with increased effort and enhanced measures should be taken.

4.1.2 Suspicious Transactions Types for Financial Institutions within the Scope of Terrorism Financing

Pursuant to Law No. 5549, obliged parties are required to report suspicious transactions to the MASAK. In this context, the MASAK has been granted the authority to prepare and publish general and sector-specific suspicious transaction reporting guidelines for obliged parties.

MASAK prepares new guidelines and periodically updates the existing ones based on sectorial risks and the latest National Risk Assessment findings in order to assist obliged parties in identifying suspicious transactions and to ensure that they adopt a common approach, understanding, and cooperation against the risk of being used as instruments in money laundering and the financing of terrorism and they report suspicious transactions in a secure, rapid and easy manner. These guidelines, which include STR types tailored for obliged parties, are announced through the official website of MASAK and/or via MASAK.ONLINE.

In this context, given below are some types of suspicious transactions identified by MASAK, in relation to individuals suspected of having links to terrorist organizations, transactions with high-risk countries, and activities related to non-profit organizations:

- Opening an account, making transfers or wire transfers on behalf of natural and legal persons known to be affiliated with a terrorist organization.
- Customer conducting a transaction, stating that he/she is making a payment or collection on behalf of persons whose assets have been frozen
- Transferring funds in amounts that have no commercial explanation or economical purpose, through wire transfer to a business account opened in risky countries and/or withdrawing such funds from the account.
- Transferring or receiving funds to and/or from risky countries, opening accounts within the financial institutions in these countries or using the credit cards issued by the banks located in those countries.
- Transfers of funds by third persons on behalf of customers by exchanging foreign currency to the countries in which terrorism and smuggling are frequently seen; or which are known as tax havens; and which have no clear business relation with the customer.
- Transferring the deposits formed in a short period of time as a result of the transfers conducted from or through risky countries to third parties.
- Collecting funds especially from/into risky countries using a high number of individual or commercial accounts and directing those funds to a small number of beneficiaries.
- The use of commercial financial transactions in fund transfers to or from risky countries without a commercial purpose making the transaction reasonable.
- The transfer of funds collected from multiple individuals under transaction descriptions like aid, support, etc., to payment institutions or virtual asset accounts.
- In mobile banking transactions, IP logins from high-risk countries or conflict zones that are inconsistent with the customer's profile.
- The customer making purchases or credit card expenditures on expensive or sophisticated communication devices or information technology (such as satellite phones, field communication equipment, etc.) that are inconsistent with their profile.
- The customer transferring funds collected from numerous individuals with transaction descriptions such as aid, support, etc., to crypto asset accounts.
- Inconsistencies between the stated purpose, activities and apparent sources of an NPO and the nature and size of its financial transactions or amount of funds raised or transferred.
- Sudden increases detected in the frequency and amounts of financial transactions in the bank account of an NPO.
- Funds kept in NPO’s account for a very long period of time.
- NPOs receiving donations only from abroad or significant ratio of donations sent from abroad.
- Directors of NPO being foreign nationals; particularly existence of transactions with large amounts carried out by the directors with their own countries; and transfers sent to high-risk jurisdictions.
- Inexplicable links of the NPO; for example, several NPOs transferring money to each other or sharing the same address, same managers or personnel.

- ❖ NPOs with no sufficient number of personnel, proper offices or telephone numbers having large account movements as if they operate intensively.
- ❖ Funds transferred from abroad to non-profit organizations being withdrawn from regions outside the operation area of the NPO.

The types of suspicious transactions determined by MASAK are of a guiding nature, and obliged parties should not limit themselves to these predefined types when identifying suspicious transactions; they should file a Suspicious Transaction Report (STR) even if the transaction raising suspicion does not match any of the listed types.

4.2 Case Studies

Case 1: An attempt to Transfer Funds to a Person whose Assets have been Frozen
Abused Sectors: Bank, Crypto Asset Service Provider (CASP)

Mr. B ordered a fund transfer to Mr. A who was among the listed persons (list of Terrorist Organisation X) about whom asset freezing decisions were made regarding their assets in Türkiye with the "Asset Freezing Decision" of the Ministry of Treasury and Finance published in the Official Gazette. Bank Y did not carry out a transaction and reported the case to MASAK.

A MASAK analysis about Mr B. revealed that an STR had previously been sent about him by a CASP stating that he had carried out high-volume crypto asset transactions.

Findings of Analysis:

According to the research done through Social Security Records Mr. B had no records of employment or registration. Research through Revenues Administration records revealed that he had no declarations of any occupation.

Examination of other records accessed by MASAK demonstrated that all bank accounts of Mr. B were in Bank A. He had no other bank accounts in any of the banks in Türkiye.

According to the banking transactions records, Mr. B sent a total amount equivalent to 1.023.754 TL to 87 different persons whose customer identification could be done between 2019 and 2021. In the same period of time, he also received a total amount equivalent to 1.474.036 TL from 143 different natural and legal persons whose customer identification could be done.

Some explanations stated in transfers he received included expressions that gave the impression that donations made with religious purposes had been abused.

Banking transactions records pointed out that there were 216 natural and legal persons whose customer identification could be made who were parties of Mr. B's transfers carried out between 2019 and 2021. MASAK research on these 216 persons disclosed that 56 of them has criminal records due to "being member of armed terrorist organisation".

Mr. B's account movements within the CASP were analysed and two types of transactions were detected:

- Transactions for transferring crypto assets sent regularly to Mr. B's crypto wallet by unknown persons to bank account after changing them into TL usually on the same day
- Transactions for transferring the amounts in TL sent to Mr. B' CASP account to wallets belonging to unknown persons by changing them into crypto assets.

The Information Note written depending on the analysis was sent to Turkish National Police (TNP). TNP found out that Mr. B had connections with conflict areas and intermediated in international fund transfers towards foreigners kept in camps located in these areas, and used

crypto assets for ensuring confidentiality in such transactions. All these determinations were combined and sent to the Public Prosecutor.

The Public Prosecutor made an indictment of TF crime and prosecution was initiated against the person.

Case 2: Provision of In-Kind Support to a Terrorist Organization through Financial Leasing

Abused Sectors: Bank, Insurance Company, Financial Leasing Company

According to an STR received by MASAK from a financial leasing company, the obliged party visited a company with which they had a financial leasing business for a construction vehicle since there had been a delay in payments and they could not contact with company officials. During that visit neighbours of the company told that a truck had come in front of the company and all the equipment was taken away, and that they had not seen anyone of the company officials since then. Afterwards, GPS records showed that the equipment had lastly been in an area close to conflict regions. The plate number of the truck that had come for transporting the company's goods was detected thanks to the security cameras of the neighbouring shops. Since the obliged party suspected of TF offence, they submitted an STR to MASAK.

MASAK analysis disclosed that the trucks registered owner Mr A had previously been the subject of an STR received by MASAK submitted by an insurance company. That STR suggested that Mr A was the insured party of policy of Turkish Catastrophe Insurance Pool (TCIP) the insurant of which had been Mr B, about whom there had been a decision of freezing of assets due to TF.

Further, fund transfers of company officials were examined. It was found out that funds sent into their accounts from abroad were transferred to the accounts of different resident people who had UYAP (Judicial) records due to crimes of being member of armed terrorist organisation, making the propaganda of the terrorist organisation or its purpose, smuggling of migrants, trafficking of or supplying narcotics or psychotropic substances. The case was forwarded to TNP with a suspicion of TF.

The HTS (Historical Traffic Search) and base analyses of TNP disclosed that Mr A's mobile phone had lastly had signals in an area close to conflict areas and on the same day he had had a telephone contact with Mr C who was the former mayor of Municipality X and had been discharged from office since there had been an investigation about him due to being a member of terrorist organisation. Communications of Mr A and Mr C were recorded during the following technical surveillance. During these communications they admitted that the abovementioned equipment was delivered to the terrorist organisation.

All the detections of MASAK and TNP were combined and sent to the Prosecutor.

The public prosecutor accepted the mentioned financing activities as reasons aggravating the terrorist organisation membership, and drew up an indictment accordingly.

Case 3: Provision of Financial Support to Members of Terrorist Organizations Detained in Prisons

Abused Sectors: Bank

Mr A opens an account in Bank X by stating that he carried out shuttle trading in his country with goods he bought from Laleli. Mr A carried out a few transactions through his account but he received a great number of transfers from different countries.

Bank X examined Mr A's account movements and transfers, transfer message samples, photocopy of his passport and customer information form. After detecting that the customer's transactions were incompatible with the information he gave while opening the account, the Bank X submitted an STR to MASAK.

After a short period of time following the submission of STR, Mr A's brother Mr B opened an account in the same branch of the same Bank. He told bank officers that he wanted to withdraw the funds in his brother's account using a power of attorney. Bank officers examined the power of attorney and observed that it had been given from prison. They asked Mr B about his brother and he gave conflicting answers such as "he was away for travel" or "he was slandered and imprisoned". Then the Bank submitted an additional STR together with identity information, a copy of the power of attorney and the customer information form.

MASAK carried out a research and found out that:

- Mr A was punished with imprisonment due to being member of terrorist organisation but Mr B did not have any criminal records,
- Mr A collected numerous transfers he'd received in his account,
- These persons received several transfers on their names other than those they received in their accounts.
-

Detailed research on fund transfers they received on their names and in their accounts revealed that:

- Most of the transfers were from different persons residing in 9 different countries in Europe, and some of these persons had been subjects of STRs submitted by different payment institutions with suspicion of affiliation with terrorism;
- Mr A and Mr B withdrew the funds they'd received in cash and they transferred them to other people residing in Türkiye.

The beneficiaries of these transfers were investigated and it was understood that either they or some of their family members had records of investigation and prosecution due to membership, aiding a terrorist organisation or making propaganda of terrorist organisation.

The research demonstrated that the transactions carried out with Bank X may constitute the TF offence. The case was forwarded to the relevant Chief Public Prosecutor.

Case 4: Provision of Financial Support from Abroad to Members of Terrorist Organizations and Their Families for Adherence to Organization

Abused Sectors: Bank, Payment Institution

According to an STR submitted to MASAK by a payment institution, **Mr A** who was wanted for being one of the directors of Fetullahist terrorist organisation attempted to make a transfer of 1000 USD in 2022 via a payment institution from Europe to **Mr H** residing in Türkiye. However, since there was an asset-freezing decision taken in 2021 against Mr A, the transfers were not carried out.

Afterwards, MASAK did an examination and found out that 2 years ago Mr A transferred 3000 USD from Europe to Mr H through a payment institution.

It was also detected that Mr A made other transfers of 10.000 TL in 2018, 20.500 TL in 2019 and 35.500 TL in 2020 to Mr H via Bank X internet banking.

In the course of MASAK analyses, another STR was received stating that **Ms C** who was residing in the same address as Mr A in Europe transferred 1000 USD to Mr H via a payment institution.

MASAK determined that Ms C was Mr A's sister and Mr A tried to transfer funds using her name since there was an asset freezing decision about him.

The analysis on **Mr H** showed that:

- In May 2022, he was registered in the social security system as an employee of "XYZ Technology Ltd."
- He had no UYAP (judicial) records
- In 2020 and 2021, he made 8 transfers ranging from 2000 TL to 3000 TL with the transaction description as "Name Surname: DDD, TR ID No:88888888, Prison X".
- The person DDD had UYAP records of various crimes such as aiding terrorist organisation and trafficking of drugs.

MASAK drew up an information note on **Mr H** and disseminated it to judicial authorities and TNP. The Police wiretapped Mr H within the framework of an investigation. It was detected that he had some conversations about the imprisoned terrorists and their families. A lawsuit was brought about him.

Case 5: Financing of Terrorism Through Cardless Transactions

Abused Sector: Bank

According to an STR submitted by a bank:

Person A told that he wanted to deposit money into his account with cardless transaction using the ATM at Bank X's branch. The security of the branch suspected of him and it was then understood that he was not the actual owner of the account. The Bank made a research

and detected that Mr A's address was registered in another city and he was trying to deposit money to Mr B's account, and reported the case to MASAK.

The examination done by MASAK revealed that he carried out the mentioned transaction via a bank which did not require a confirmation code, and that the account owner had UYAP records due to being a member of terrorist organisation. The case was forwarded to judicial authorities with a suspicion of TF.

The investigation initiated by judicial authorities covered other persons who had connections with A and B and reached a total of 154 persons. It was detected that the terrorist organisation used cardless ATM transactions as a method of sending funds to its members. Lawsuit was brought about the persons due to TF crime.

Case 6: Provision of Financial Support from Abroad to Members of Terrorist Organizations and Their Families for Adherence to Organization

Abused Sector: Payment Institution

An STR received by MASAK specified the following information:

Mr. M who had declared that he was working freelance received a total of 15.800 USD from Mr. A through 15 international fund transfers between 2020 and 2022. Mr. M also received 530 EUR through 4 transactions and 1.800 USD through 5 transactions from 6 different persons in countries X, Y and Z in the abovementioned period.
The amounts of the transactions ranged between 200 USD and 900 USD and all of the transactions were from 2 different payment institution agents in İzmir/Gaziemir and İzmir/Konak.

The TF examination by MASAK revealed that there was media news reporting that a Mr. A who was wanted for being a member of the Fetullahist Terrorist Organization was living at an address close to the region where the leader of Fetullahist Terrorist Organization was known to be living.

In conformity with the media news, Mr. A who was the originator of the aforementioned transactions had made the transfers from an address close to the region where the leader of Fetullahist Terrorist Organization was known to be living.

MASAK analysis showed that Mr. M did not have any criminal records. It was also found out that Mr. M sent the amounts he had received from Mr. A to Miss K on the same day or the following days.

Inquiries into Miss K did not reveal any criminal record against her. However, it was found that her husband and three of her brothers were convicted and were in prison for being a member of an armed terrorist organization.

An information note was prepared about the case and was disseminated to judicial authorities and the TNP by MASAK as it was suspected that the case could be linked to financing of terrorist organization.

Case 7: Financing of Terrorism through Cash Deposits and Electronic Marketplace Platforms

Abused Sectors: Bank, Payment Institution, CASP, Electronic Commerce Intermediary Service Provider (ECISP)

An STR received by MASAK specified that Mr. A had a foreign currency account opened in the name of his mother with Branch Y of Bank X, and various amounts of money was deposited into this account starting from the day following the account opening date. Besides, the last request of deposit into account involved ciphered banknotes of the Fetullahist Terrorist Organization and it seemed like the banknotes had been hidden for a long time as they were dirty and had a mouldy and earthy smell. The inquiries into the suspect, who wanted to conduct those transactions for the benefit of his mother Mrs. B whose access to banking services and knowledge in this field is supposed to be low due her age, revealed various social media profiles, blogs and individual e-commerce websites of the suspect.

It was found that in his blog, the suspect displayed the banknotes he wanted to deposit in the bank by giving the impression that he was a collector, and he put various paintings on sale on his personal e-commerce platform account. The paintings, in general, did not any have value as collection pieces; however, they were listed at very high prices.

Inquiries into banking transaction records of Mr. A revealed that his account with an electronic payment institution received transfers from various persons. The amounts received were immediately transferred to a local crypto-asset service provider and were right away converted to crypto assets and transferred to another wallet whose owner could not be identified.

Moreover, while Mr. A was attempting to conduct the transaction at branch (Y) of Bank (X), there was a child of foreign nationality with him and he called Mr. (A) as father. The inquiry into Mr. A revealed that he was married to a foreign woman and considering that the organization was quite active in African counties, the case was found suspicious.

Taking all this information into account, it was suspected that Mr. A could be financing terrorism, and therefore, the report was referred to judicial authorities.

Case 8: Financing of Terrorism through Cryptoassets Transfers

Abused Sectors: CASP, Bank, Association

Public Prosecutor's Office initiated an investigation based on the information that there was an attempt to illegally provide financial support to DAESH by receiving cryptoassets and transferring them to conflict zones to rescue DAESH members imprisoned/ held captive in those zones.

Wiretapping and technical surveillance conducted in the investigation revealed that organizational meeting were being held at so-called madrasahs, where people were urged to make donations to so-called madrasas and associations affiliated with the organization and recruitment activities for carried out for the organization.
The information acquired from MASAK set forth that the suspects had conducted inexplicable, high-amount fund transfers inconsistent with their financial profiles; those fund transfers were more frequent in certain periods; there were high amount cash deposits into bank accounts in single transactions, which were later transferred to crypto exchanges;

transaction descriptions of the transfers specified suspicious statements; and the suspects frequently conducted transactions with persons that were processed for terrorism offence and that were subjects of asset-freezing decisions. Activities conducted in coordination with MASAK for the identification of the users of 26 crypto wallets revealed that a total of 80.000 USD received from various wallets was transferred on the same day to a crypto wallet in a foreign country believed to be affiliated with the terrorist organization. Those transfers were conducted using coins known for enabling anonymity and privacy. Inquiries into crypto wallets of the subjects revealed that funds were received from different wallets, and then, they were sent to joint wallets incorporating wallets used for collecting donations for DAESH through internet-based texting channels operating on behalf of DAESH.

Within the scope of the investigation, operations were conducted in 5 cities and 49 individuals were captured and put into custody. One cold wallet, around 1 million TL worth of cash and gold, a large number of banned books on the organization and digital materials and documents were seized in the searches conducted in the residences and so-called madrasahs of the suspects. The digital materials depicted visuals of the so-called caliphate flag of DAESH, videos of armed DAESH members at DAESH camps, and data on internet-based instant messaging groups where organizational communications were exchanged.

Inquiries into the Association A.B revealed that the organization was in search of recruits for DAESH, conducted activities to instil the organization's ideology in its sympathizers, and carried out the financing activities of the organization. Upon these findings, the association and the so-called madrasahs illegally-operating in four locations were closed down.

The suspect Mr. X wished to benefit from the provisions of effective repentance and gave a statement revealing that Mr. M who was in Country A was the media coordinator of DAESH and he managed some messaging groups affiliated with the organization. Those group chats were used to provide training on how to transfer cryptoassets to accounts shared by Mr. M to be used for the people held at camps in Syria and DAESH members. For this purpose, accounts were opened with cryptoassets service providers and people were instructed to conduct the transactions using anonymity-enabling coins in order to conceal the source of the funds collected.

Case 9: Financing of Terrorist Organization through Social Media

Abused Sectors: Bank, Payment Institution

LEAs initiated an investigation in 2021 upon the finding that foreign national Mr. A asked people over social media to send funds to his bank accounts.

Financial analysis of MASAK revealed that the subject's account received a total of 11.817.647 TL in 1.857 transactions and sent 11.355.539 TL to various accounts between 2017-2019. It was found that he received money transfers through banking and payment institution channels from his contacts located in various countries across Europe. Mr. A's assets were frozen in 2021 under Article 7 of Law No. 6415 for suspicion of Al-Qaida and DAESH affiliations.

Mr. A was apprehended in an operation conducted in 2021 and numerous terrorist organization-related digital materials were seized in his residence. Upon the findings acquired thereon, operations were conducted in 9 provinces to targeting 11 suspects.

As a result of the judicial process, Mr. A was sentenced to 5 years of imprisonment for financing of terrorism under Law No. 6415.

Case 10: Financing of DAESH through Digital Hawala Applications
Abused Sector: Bank

An investigation was initiated due to violation of the Law No. 6415 on the Prevention of the Financing of Terrorism based on the information that Mr. A collected funds from the foreign nationals residing in his town and transferred them to DAESH via banks or various digital hawala applications

The financial analysis of MASAK revealed that Mr. A had 784.639 TL of fund transfer relationships between 2017 and 2022 with 22 persons who had criminal records for being member of a terrorist organisation (DAESH). He also had transfer relationships of a total amount of 2.261.338 TL with 3 persons assessed to be serving as hawaladars in the hawala system. He had had transfer relationships of a total amount of 2.703.981 TL with 4 persons whose assets were afterwards frozen for being member of DAESH terrorist organisation. Other detections about Mr. A are as follows: He carried out financial transactions that were incompatible with his professional profile; although he did not have any company partnership with the persons, he frequently carried out high amount transfers with them. The explanation sections of transfers were left blank without any explanation. People transferred low amounts not to attract attention but the transfers were repeated many times. Beside transfers, Mr. A carried out cash deposit and withdraw transactions, transferred the deposited and/or received funds to different people on the same day and/or withdrew them as cash. He usually used ATMs and Internet banking.

Within the scope of the inquiries into Mr. A and 71 persons with whom he had fund transfer relationship, the major suspects Mr. A, Mr. B and Mr. C. were wiretapped and surveilled through technical tools. It was found out that the three suspects carried out hawala activities in the region, they talked about hawala transfers during the calls they received through their mobile phones. Then, as an organisational behaviour, they directed the people calling to web based texting applications to avoid being wiretapped.

During the investigation, operations were conducted in several cities and 150.000 TL, 11.000 USD, 600 Euro and digital materials were seized in the operations. The preliminary examination of the digital materials and the statements of suspects revealed that there were digital hawala applications downloaded through the links sent by someone else to provide funds to the terrorist organisation.

Case 11: Financing of Terrorism through Apparently Legal Activities
Abused sectors: Bank, Payment Institution

An investigation was initiated into a structure that was found to carry out financing activities on behalf of PKK/KCK-PYD/YPG, provided financial support for the families of terrorists who died or were imprisoned, and organised charity and donation campaigns in 13 different

countries using crowdfunding method additionally under the name of non-governmental organization.

The coordinated research revealed that this structure was composed of interlinked associations in 13 countries with similar names and emblems; most of the related persons were members of associations in Türkiye affiliated with PKK/KCK-PYD/YPG, and they had family members who were imprisoned for being member of PKK/KCK-PYD/YPG or who died during armed conflicts.

MASAK analysis found out that this structure sent 2.5 million Euros from 2010 to more than one thousand people in Türkiye.

Case 12: An STR with a Suspension Request Involving an Individual whose Assets have been frozen

Abused Sectors: Bank

Bank M filed an STR with a suspension request under Article 19/A of Law No. 5549 in relation to withdrawal of the balance of 9.638 TL and 2,28 USD held in Mr. Z's account. The bank filed the STR due to Mr. Z's intensive transactions with Mr. X whose assets were frozen in 2023 for being affiliated with DAESH.

It was decided, with the approval of the Ministry, to suspend the aforementioned transactions for 7 (seven) business days in accordance with Article 19/A of Law No. 5549.

MASAK analysis conducted for confirming the suspicion that the assets in question were linked to the financing of terrorism and for examining the transactions revealed that Mr. Z and Mr. X were partners of the Company T and there were a large number and volume of transactions between these two people before Mr. X's assets were frozen.

The findings acquired from the analysis were forwarded to Public Prosecutor's Office for judicial assessment.

Case 13: Financing of Terrorism through Social Media and Cryptoasset Transfers

Abused Sectors: CASP

A CASP filed an STR to MASAK, specifying that there was a call for support on a social media account of the separatist terrorist organization, the terrorist organization was seeking to procure "drones" to use them in terrorist attacks, and it shared cryptoassets wallet account information on social media platforms to find funds for this purpose.

MASAK analysis into wallet addresses shared social media accounts and acquired through open sources identified transfers to these wallets made through CASPs operating officially in Türkiye. In this scope, it was found that cryptoassets with a total worth of 20.000 USD were collected in 6 crypto wallets. 9 individuals were identified by use of those crypto asset transfers.

After the inquiries, it was concluded that the transfers conducted through CASPs may constitute the offence of financing of terrorism, and therefore, the case was referred to the Public Prosecutor's Office.

Case 14: A TF-related STR with a Suspension Request

Abused Sectors: Bank, Payment Institution

Bank X filed an STR to MASAK with a suspension request under Article 19/A of Law No. 5549 for the suspicion of financing of terrorism. The STR was filed because Ms. A who was on the grey list of the Ministry of Interior for being wanted for being a member of the terrorist organization "DHKP/C" was recently granted a retirement pension by the Social Security Institution and the balance deposited into her account as retirement pension was attempted to be withdrawn by Ms. B, the daughter of Ms. A, using a power of attorney issued in a foreign country.

It was decided, with the approval of the Ministry, to suspend the aforementioned transaction for 7 (seven) business days in accordance with Article 19/A of Law No. 5549.

MASAK analyses revealed that Ms. A had arrest warrants, prosecution and investigation records for the offence "being a member of an armed terrorist organization", Ms. B had received fund transfers from Ms A through a payment institution, Ms. B also received other fund transfers from abroad through the payment institution and the originators of those transfers had arrest warrants, prosecution and investigation records for the offence "being a member of an armed terrorist organization.

After the inquiries, a report was written about the transaction suspended pursuant to Article 19/A of Law no 5549. The report specified that the suspicious transaction reported to MASAK with a suspension request was about the retirement pension granted to Ms. A by the social security institution, and the transaction was suspended taking into account that Ms. A was on list of persons wanted for terrorism offences, she had an arrest warrant for the offence "being a member of an armed terrorist organization, the funds in question could possibly be used for financing of terrorism upon being transferred to Ms. A or other people designated by her, her daughter Ms. B could be acting as an intermediary for such acts, and the a suspension could coerce Ms. A to cease being a fugitive. The report written was referred to Public Prosecutor's Office to be evaluated in terms of TF offence under Law No. 6415 and Article 248 titled '*Coercive Seizure and Guarantee Document*' of Criminal Procedure Law No. 5271, which stipulates '*To ensure that the fugitive applies to the public prosecutor or attends a hearing, his or her property, rights, and receivables in Türkiye may be seized, proportionately to the purpose, upon the request of the public prosecutor, by a criminal judge of peace or by court order. If necessary, a trustee shall be appointed to manage the property. The decision to seize and appoint a trustee shall be notified to the defence counsel*.'

5. CONCLUSION

It is known that the objective of terrorist organisations is not earning money as it is the case in organised crime organisations, but it is clear that they need financial support in order to perform their organisational and ideological activities. Terrorism constitutes a great threat against international peace and security, and no terrorist act can be accepted as legal no matter where, when or by whom it is perpetrated. Türkiye is a member of FATF, which is a global anti-money laundering and counter terrorist financing organisation. In order for full compliance with FATF recommendations Türkiye constantly revises its legislation and practices of CFT. Besides, as terrorism is the most significant threat against the national security of the Republic of Türkiye, the financing of terrorism is a problem with the same level of importance.

Years of terrorist activities and security forces' fight against these activities led to the change and evolution in methods of terrorist organisations for getting financial support. The development of new technologies and digitalisation of financial transactions particularly after the years 2000s have created new instruments on one hand and new responsibilities of supervision regarding the funds used for TF, on the other. The most important stakeholders of this responsibility are financial institutions, DNFBPs and other entities that can be possibly used as intermediaries by terrorists or their financers due to the services they provide. They are specified as "obliged parties" in legislation.

Within this framework, duties and responsibilities of entities listed as "obliged parties" in the Law No. 5549 on Prevention of Laundering Proceeds of Crime and the Law No. 6415 on Prevention of Financing of Terrorism and their secondary legislation are critically important in the fight against TF.