

FINANCIAL MONITORING
AGENCY OF THE REPUBLIC OF
KAZAKHSTAN



NATIONAL RISK ASSESSMENT OF THE FINANCING OF TERRORISM AND PROLIFERATION OF WEAPONS OF MASS DESTRUCTION

Public report

2021

STRUCTURE OF THE REPORT
on the national risk assessment of the Republic of Kazakhstan

Summary.....	2
Chapter I. Introduction.....	3
Chapter II. Threats and risks of terrorism financing.....	8
Chapter III. Identifying FT Vulnerabilities and Risks for NPOs.....	9
Chapter IV. Vulnerabilities and risks of FT for the financial sector.....	10
1. FT Vulnerabilities from the use of cash and payment cards.....	11
2. Vulnerabilities of FT in intermediary services in sale and purchase of immovable property.....	12
3. Vulnerabilities from the use of digital assets.....	13
Chapter V. Threats, Vulnerabilities and Risks of FPWMD	14
Chapter VI. Conclusion on the risks of FT, FPWMD.....	15

SUMMARY

The national system functioning in the Republic of Kazakhstan for combating the financing of terrorist activity and the financing of proliferation of weapons of mass destruction (hereinafter - NS FT/FPWMD) promotes strengthening of national security and stability of the financial sector.

National risk assessment of terrorism financing and financing of proliferation of weapons of mass destruction (hereinafter - FT/FPWMD) is conditioned by the requirements of the Financial Action Task Force (hereinafter - FATF) standards, in order to update the areas of illegal activities, which should be given priority attention, as well as to identify the most vulnerable areas of NS FT/FPWMD, identified during the first national risk assessment in 2018.

The tasks of the national risk assessment equally include updating and researching the existing threats, vulnerabilities of the NS FT/FPWMD and risks arising from it, understanding the processes taking place in the system, and identifying potential initiatives for its development.

The national risk assessment of FT/FPWMD was carried out by the Financial monitoring agency (hereinafter - FMA) with involvement of participants of the NS FT/FPWMD, including 18 state, law enforcement and special state bodies and private sector organizations, being the subjects of financial monitoring, which allowed making a versatile analysis of the existing situation in the sphere of FT/FPWMD in the Republic of Kazakhstan.

As part of the national risk assessment, the analysis of data, information and criminal legal statistics for the period from 2018 to 2020 was conducted. Data collection was carried out on the basis of the Methodology on data collection from state bodies and subjects of financial monitoring to assess the risks of money laundering and terrorism financing by organizations, approved by the Order of the Minister of Finance of the Republic of Kazakhstan № 196 of March 29, 2017.

National risk assessment will provide an opportunity to take necessary management decisions promptly and in a certain sequence in relation to threats, vulnerabilities and in general the risks of FT/FPWMD, which will allow to take measures to minimize them and, as a result, to improve the effectiveness of the NS FT/FPWMD of the Republic of Kazakhstan.



Chapter I. INTRODUCTION

The national system functioning in the Republic of Kazakhstan for combatting terrorism financing (hereinafter - NS CFT) contributes to strengthening of national security and stability of the financial sector. In connection with the existing terrorist threat faced by the whole world community, the necessity of deep understanding of factors, determining presence and occurrence of cases of financing of terrorism (hereinafter - FT) in the state, comes to the fore.

The National Risk Assessment of Terrorism Financing (hereinafter - NRA FT) is required by the FATF standards in order to identify areas of illegal financial activity, which should be given priority attention, as well as to identify the most vulnerable areas of NS CFT.

The NRA FT was conducted by the FMA with the involvement of participants of NS CFT, including state, law enforcement and special state bodies, the National Bank, which allowed to make a comprehensive analysis of the current situation in the sphere of combating FT in the Republic of Kazakhstan.

The results of the NRA FT will be recommended for consideration in law enforcement practice when choosing specific measures to minimize certain risks of terrorism financing and in the allocation of resources at all levels of the NS CFT.

The goal of the NRA FT is to identify the riskiest methods and tools used by terrorists or terrorist groups in the Republic of Kazakhstan to raise, move or use funds for criminal purposes. The tasks of the NRA FT equally include the study of existing threats, vulnerabilities in the NS CFT and the risks of FT arising from it, understanding the processes taking place in this system, as well as identifying potential initiatives for its development.


The NRA FT will provide the opportunity to make the necessary management decisions promptly and in a certain sequence, in relation to the threats, vulnerabilities and risks of FT in general, which will improve the effectiveness of combating FT in the Republic of Kazakhstan.


Assessment of FT risks is carried out in accordance with the stages of the terrorism financing process, through which the ways of attracting, moving or using funds are determined.

STAGES OF THE TERRORIST FINANCING PROCESS

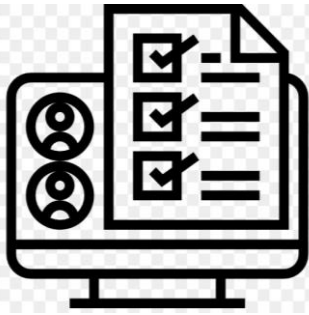
RAISING FUNDS	The initial stage of the FT process, the main purpose of which is to raise funds from both legal (examples: private donations, collection through NGOs, businesses, etc.) and illegal (examples: proceeds from criminal activity, etc.) sources.
MOVEMENT OF FUNDS	The technical phase of the FT process, the main purpose of which is to engage legal and/or illegal mechanisms for the movement of terrorist funds (examples: money transfers through banks, cash transportation, etc.).
USE OF FUNDS	The final stage of the FT process, the main purpose of which is to use funds to support all activities carried out by terrorists or terrorist groups (examples: conducting terrorist acts, propaganda and recruitment, education and training, etc.).

KEY CONCEPTS OF THE NRA FT

<p>THREAT</p> 	<p>To identify the threat, two questions must be answered: "who?" and "how?" In the case of FT, the answer to the question "who?" is a person or group of persons with the potential to cause harm to the state, society, economy, etc. It should be noted that the person or group of persons can be both known (for example, included in the List of organizations and individuals in relation to whom there is information about their involvement in extremist activity or terrorism (hereinafter - the List), or unidentified persons or group of persons.</p> <p>The answer to the question "how?" will be the ways in which funds are raised, moved or used.</p> <p>The threat is assessed on the basis of the following factors:</p> <ul style="list-style-type: none"> - the likelihood of terrorists or terrorist groups using the method; - the ability of the terrorists or terrorist groups to use the method (example: the availability of the necessary expertise); - statistics of how terrorists or terrorist groups use the method.
--	---

<p>VULNERABILITY</p>	<p>To determine vulnerability, it is necessary to answer the question of why terrorists or terrorist groups use this method.</p> <p>The answer will be the combination of availability and visibility of the means to attract, move or use the funds, at which they can be used to carry out the threat.</p> <p>That being said:</p> <ul style="list-style-type: none"> - accessibility of the method - the convenience and ease of use of the method for the purposes of FT; - visibility of the method for the participants of the NS CFT - the extent to which the method is regulated by the national legislation or is influenced by the other measures, including detection in the implementation of operational activities.
<p>CONSEQUENCE</p>	<p>The consequence of FT is the answer to the question "what will it lead to?", namely, the terrorist manifestation itself.</p> <p>Given this fact, we believe that the consequence is a constant value, based on an assessment of the potential for the attraction and movement of funds:</p> <ul style="list-style-type: none"> - for operational purposes - the use of funds to directly carry out a specific terrorist manifestation (examples: terrorist attack, movement of fighters, and preparation of an attack); - for organizational purposes - the use of funds to meet the needs and maintenance of a terrorist group (examples: recruitment, training, maintenance of training camps, radical centers).
<p>RISK</p> 	<p>Considered as a function of three factors: threat, vulnerability and consequence in the following formulation:</p> <ul style="list-style-type: none"> - The likelihood that terrorists or terrorist groups will employ a method of raising, moving, or using money because of a number of circumstances (availability and visibility) that lead to terrorist manifestations.

PRIORITIZATION



Prioritization is an assessment of the sequence of risk management measures in relation to time.

Risks for which it is essential to take measures to minimize them as soon as possible belong to the group of **high-level risks**.

Risks that need to be monitored and, if necessary, containment measures need to be taken are in the **medium-level risk** group.

Risks that have the potential to develop and therefore a work to minimize them need to be started belong to the group of **low-level risks**.

The risk assessment-based approach opens up new perspectives for both the public and private sector. It requires the pooling of all resources and expertise to collect and properly interpret risks information, both at the country level and at the level of individual organizations, to develop procedures and systems, and to train staff accordingly. The process involves confirming the existence of risk and developing strategies to manage and mitigate the risks identified.

It should not be assumed that the assessment made at any particular stage will remain unchanged. The situation may change over time, depending on how events develop and what new threats emerge. This approach can be implemented in many different forms, resulting in a systematic updating of the approach and a more accurate compliance with the established requirements.

THREAT ASSESSMENT MATRIX

Threat level report	
High	repeated facts of committing an unlawful act of terrorism financing, its possibility and safety in terms of low level of disclosure, availability of technical and financial, etc. opportunities for committing an unlawful act.
Medium	existence of facts indicating attempts to commit or the commission of terrorism financing, or the commission of such an unlawful act is extremely difficult or extremely dangerous in terms of the high level of detection and punishability of crimes, the presence of technical and financial and other opportunities to commit terrorist financing.
Low	absence of facts, persons who have intentions to commit an unlawful act aimed at terrorism financing, or committing such an unlawful act is extremely difficult or extremely dangerous in terms of the high level of detection and punishability of crimes. There are no technical, financial, etc. possibilities for committing terrorist financing.

VULNERABILITY ASSESSMENT MATRIX

Vulnerability level report	
HIGH	method is used by terrorists or terrorist groups for FT purposes due to the high level of availability and medium or low visibility.
MEDIUM	method can be used by terrorists or terrorist groups for FT purposes due to a certain level of aggregate accessibility and visibility.
LEVEL	it is almost impossible for terrorists or terrorist groups to use the method for FT purposes due to the required level of aggregate visibility and accessibility.

RISK ASSESSMENT MATRIX

THREAT				
		Low	Medium	High
Vulnerability	High	Medium	High	High
	Medium	Low	Medium	High
	Low	Low	Low	Medium
Vulnerability level report				
HIGH	the risk is a major risk and requires close attention. The method is very attractive for FT purposes. There are indications that funds are being raised or moved with significant consequences.			
MEDIUM	the risk is moderate, but may require increased attention and further elaboration. The method may be interest to terrorists or terrorist groups. There are indications that funds are being raised or moved for FT purposes.			
LOW	the risk is acceptable, but needs to be carefully monitored, also it may be a potential risk. The method may be attractive to terrorists or terrorist groups. There is little or no evidence of the solicitation or movement of funds for FT purposes.			



Chapter II. THREATS AND RISKS OF TERRORISM FINANCING

The main threat of terrorism financing in the Republic of Kazakhstan comes from the following persons or their groups, which use or may use one of the methods of raising and using funds for TF purposes:

1. adherents of non-traditional (destructive) religious movements, followers of new trends in Islam - marginalized individuals receiving distorted information from the Internet, as well as in various messengers;
2. citizens of Kazakhstan, independently traveling to receive theological education abroad, including countries with terrorist activity;
3. citizens of Kazakhstan traveling to areas of heightened terrorist activity in order to join international terrorist organizations, as well as returning from said areas;
4. members of terrorist organizations, illegal armed groups and radical groups located outside the territory of the Republic of Kazakhstan and engaging Kazakhstani citizens in terrorist activities via the Internet.

Risk factors. The means received from legitimate sources are used at financing of terrorism: with use of transactions on non-cash bank transfers, with use of bank plastic cards, services of payment organizations (money transfers without opening an account), and also criminal incomes, including legalized ones. The possibility to use virtual assets for the mentioned purposes is still relevant.

Recommendations. Law enforcement and special state agencies are recommended to continue to conduct special operations, as well as participation in special international events.

Special attention should be paid to reconciliation of departmental reporting on cases related to terrorism and extremism financing.

It is necessary to constantly conduct professional development of law enforcement and special state bodies regarding counteraction to terrorism financing, including new forms, schemes and methods of terrorism financing, especially use of virtual assets, taking into account the best practices of investigation of such cases.

It also seems advisable to strengthen interaction of law enforcement and special state agencies with persons engaged in financial transactions through FMA resources (development of guides, typologies, etc.).



Chapter III. IDENTIFYING VULNERABILITIES AND RISKS OF FT FOR NPOs

There are clearly regulated procedures for establishing and monitoring activities of NPOs operating in the country, allowing them, on the one hand, to freely carry out their tasks and, on the other hand, to prevent their possible involvement in unlawful activities.

The risks of using NPOs for FT purposes are primarily related to the possibility of accumulation and/or transfer of cash. NPOs often use insufficiently controlled ways to collect donations: by depositing money into the NPO's cash register or account, donating to piggy bank boxes, using bank cards, mobile applications, and donating through intermediaries, where intermediaries may include temporary employees such as volunteers and foreign partners, who are rarely checked for trustworthiness.

In order to reduce the risks of using NPOs for FT purposes, internal controls should be further improved. At the same time, the main way to minimize the risk of misuse of NPOs for terrorism and extremism financing purposes is to control NPO expenditures in accordance with their stated goals and objectives.

The conclusion about the average threat of NPOs being used for terrorism financing purposes is also confirmed by the low frequency of detection of such facts in the practice of law enforcement and financial intelligence.

A systematic assessment of the risks of misuse of NPOs for terrorism financing purposes should continue, including in the form of separate studies aimed at preventing them from establishing connection to terrorists and terrorist groups.

In order to reduce external factors on the radicalization of the population, to improve the effectiveness of identifying and suppressing the facts of religious extremism and terrorism, including improving the system of ensuring the activities of

state bodies in the NPO sector, to amend the State program to combat religious extremism and terrorism in the Republic of Kazakhstan for 2018 - 2022.



Chapter IV. VULNERABILITIES AND RISKS OF FT FOR THE FINANCIAL SECTOR

The financial sector includes banks, exchanges, insurance organizations, professional securities market participants, organizations engaged in microfinance activities, payment organizations, postal operators providing money transfer services, i.e. whose activities in the sphere of AML/CFT are controlled by the National Bank of Kazakhstan (hereinafter - NB) and the Agency of the Republic of Kazakhstan on Regulation and Development of Financial Market (hereinafter - ARFM).

As a whole the subjects of financial monitoring, carrying out financial operations, take necessary measures of CFT: the rules of internal control are approved and carried out, risk management procedures are defined, the analysis of suspicious financial operations is carried out, information is transferred to the state body of financial monitoring.

This conclusion is confirmed by the data on the results of control measures conducted by the state bodies - regulators exercising control over the AML/CFT activities of the subjects of financial monitoring carrying out financial transactions.

The most effective CFT work is organized in the banking sector. Special units - AML/CFT compliance services - have been created in the sector, there is an understanding of the possibility of involvement in FT schemes and work is being done to manage these risks.

The subjects of financial monitoring carrying out financial operations, understand their duties on revealing the organizations and persons included in the duly formed lists of organizations and persons involved in extremist and/or terrorist activity among their clients.

The majority of subjects of financial monitoring have specialized software complexes, which allow automating AML/CFT activity. The growing number of data and information on transactions subject to financial monitoring provided by STBs indicates that there is an understanding of ML/FT risks and the need for preventive measures.

The activity of the SFM is also evidenced by the increase in the appropriate response to suspicious transactions and the preparedness of compliance officers.

The foregoing allowed to purposefully orient the activities of analytical subdivisions of the authorized body to conduct operational and tactical analyses and further referrals to the law enforcement agencies and the state security service (LEA/SSS) for implementation of verification measures.

Taking into account the provided information, the vulnerability of subjects of financial monitoring of the financial sector is assessed as medium. Risks of terrorism financing are assessed as medium.

It is recommended to introduce special criteria, developed by the authorized bodies, into the compliance procedures of financial institutions to improve the efficiency of identifying suspicious transactions in banking products possibly related to terrorist financing.

1. Vulnerabilities of FT from the use of cash and payment cards

In most cases, terrorist groups use cash for their purposes, which may come to them either legally or criminally (example: illegal cross-border movement (smuggling) of cash), and it should be taken into account that most often cash is used immediately before the preparation of a terrorist crime.

At the same time, the loss of public interest in the use of cash is also indicated by the reduction in the number of cash withdrawal-only ATMs, which continues for the third year in a row.

Risk can be minimized by implementing measures aimed at gradually reducing the share of cash in circulation.

As the level of digitalization of services increases, the population's interest in online payments and money transfers is growing. At the same time, there is a dynamic annual decrease in the number of prepaid payment cards in circulation without identification of the card holder.

The mentioned above shows the absence of FT risks, when the prepaid cards can provide the transfer between unidentified individuals, including with the intent of terrorism financing. In this regard, the degree of vulnerability to FT when using prepaid bank cards is assessed as medium.

In order to improve the efficiency of detection of bank card transactions possibly connected with terrorism financing, it is advisable to consider the introduction of appropriate special indicators.

2. Vulnerabilities of FT in the implementation of intermediary services in the purchase and sale of real estate properties.

Real estate is an attractive way to obtain cash and use it for FT purposes, as well as to provide real estate leasing services for the benefit of persons involved in terrorist activities.

Individual entrepreneurs and legal entities engaged in intermediary services for the purchase and sale of real estate (Realtors) are among the subjects of financial

monitoring. They belong to the category of established non-financial enterprises and professions according to FATF terminology.

In order to level the risk of FT, FMA conducts explanatory work with the SFM of all sectors on a systematic and regular basis. This work is carried out both through retreats to the regions and on a remote basis. In addition, each SFM receives answers to all questions of interest from the FMA through personal accounts of the "Remote Monitoring" platform.

It is necessary to take into account that in the end transactions on purchase and sale of the real estate with participation of realtors occur at notaries and in most cases with use of services of second tier banks (further - STB) where all operations and transactions get transparency on implication and possibility of use for FT, with inclusion of requirements on target financial sanctions.

Based on the above, we can conclude that the degree of vulnerability of individual entrepreneurs and legal entities engaged in intermediary services in the purchase and sale of immovable property in relation to terrorism financing is assessed as low. At the same time, the average risk of use of transactions on the sale and purchase of real estate by established persons for terrorism financing remains.

3. Vulnerabilities from the use of digital assets

On the one hand, virtual currencies such as bitcoin offer great opportunities for innovation in the financial sector. But they also attract the attention of various criminal groups and can pose FT risks. This technology allows anonymous money transfers on an international level. While the initial acquisition of the currency can be established (e.g., in the banking system), it is difficult to identify all subsequent transfers of virtual currency.

The status of digital assets in Kazakhstan was enshrined in June 2020 in the Law of the Republic of Kazakhstan "On Informatization". A digital asset is a property created in electronic digital form using cryptography and computer calculations. A digital asset is not a financial instrument, but can serve as an electronic-digital form of certification of property rights.

At the same time, the only legal tender in Kazakhstan is the Tenge. In this regard, cryptocurrencies cannot be used as a means of payment in the country.

The NB prohibits financial organizations to conduct transactions not expressly provided for by the legislation. Despite the absence of direct regulation, today the use of cryptocurrencies in the financial sector on their own or client transactions, as well as as a unit of settlement, is contrary to the law.

In view of the above, unregulated assets may be used by designated persons to finance terrorist activities.

In order to minimize the risks, it is necessary to:

- elaborate on the issue of limiting instances of payment services outside the scope of legal requirements;

- consider the issue of proliferation of the requirements of the legislation in the area of combating the financing of terrorism (hereinafter - CFT) to new financial technologies, as well as inclusion of organizations carrying out transactions with the use of cryptoassets in the number of subjects of financial monitoring.



Chapter V. THREATS, VULNERABILITIES AND RISKS OF FPWMD

Combating the financing of proliferation of weapons of mass destruction (hereinafter referred to as "FPWMD") is considered as one of the main priorities of domestic and foreign policy of the Republic of Kazakhstan.

Government, law enforcement and special agencies in Kazakhstan are constantly working to ensure the nuclear non-proliferation regime, as well as radiation, chemical and biological safety.

On the whole, the subjects of financial monitoring, which carry out financial operations, take the necessary measures to counteract FPWMD: the internal control rules are approved and implemented, risk management procedures are defined, registration of suspicious financial operations is performed, information is submitted to the financial monitoring body.

This conclusion is confirmed by the data on the results of control activities carried out by the state bodies - regulators exercising control over the activities of the subjects of financial monitoring, carrying out financial transactions, in the sphere of counteraction to FPWMD.

In order to minimize the risks of FPWMD it is necessary to improve the legislative regulation of this sphere, as well as to consider the introduction of special criteria developed by authorized bodies into the compliance procedures of financial organizations to improve the efficiency of identification of suspicious transactions, possibly related to the financing of proliferation of weapons of mass destruction.

In accordance with the updated FATF standards, in order to minimize the detected threats of the FPWMD, it is proposed to consider the criminalization of the FPWMD.

minimize the risk of abuse of NPOs for terrorism and extremism financing purposes is to control NPO expenditures in accordance with the stated goals and objectives.

The systemic risk assessment of NPOs' abuse for terrorist financing purposes should continue, including in the form of separate studies aimed at preventing them from establishing links with terrorists and terrorist groups.

Based on the results of the NRA FT, recommend the authorized bodies to consider updating the measures reflected in the state programs on combating religious terrorism and extremism, deradicalization of the population, conducting a large-scale awareness-raising work on the dangers of terrorism financing and terrorist activities.

Given the ways and forms of terrorism financing, including the use of funds obtained from legitimate sources and NPOs, law enforcement and special state bodies should continue to improve the methods of conducting parallel financial investigations, including the use of FMA capabilities.

Consideration should be given to introducing special indicators developed by the authorized bodies into the compliance procedures of financial organizations to improve the efficiency of identifying suspicious bank card transactions possibly linked to terrorism financing.

In order to minimize the risks of using other unregulated financial instruments for FT purposes, it is necessary to:

- regulate the issues related to cryptocurrency (concept, status: money, commodity or securities; legality or illegality of its use) by law;
- work out the issue of limitation of cases of payment services rendering beyond legal requirements;
- consider the issue of extending legislative requirements in the CFT area to new financial technologies, as well as inclusion of organizations carrying out operations with the use of cryptoassets into the number of subjects of financial monitoring.

The work carried out on NRA FPWMD allowed to identify the key threats, vulnerabilities and risks which are characteristic of NS CFPWMD.

It was found that the state, law enforcement and special bodies are working to ensure the nuclear non-proliferation regime, as well as ensuring radiation, chemical and biological safety, and SFM engaged in financial transactions are taking the necessary measures to counteract the FPWMD.

According to the results of the NRA, the risk level of the FPWMD is defined as medium.

FPWMD risk factors.

The presence of risk factors of FPWMD in Kazakhstan is associated with the following components:

- the geographic and regional proximity of countries such as Azerbaijan, Armenia, Afghanistan, Iraq, Iran, India, China, DPRK, Pakistan, and Syria, where there has been high military activity over the past forty years;

- Iran's nuclear program. As a member of the Treaty on the Non-Proliferation of Nuclear Weapons, Iran has been found to be in non-compliance with the provisions of the Treaty and is active in uranium enrichment and nuclear technology development. According to the International Atomic Energy Agency, Iran is storing 12 times more enriched uranium than it is allowed by the agreement between Iran and the P5+1 countries. It is possible that companies of foreign jurisdictions may use Kazakhstan as a transit zone for the movement of banned goods;

- proceeds from criminal activities, organized criminal organizations (OCGs and criminal communities) can possibly be used to finance the development and proliferation of weapons in conflict zones, including WMD.

In Kazakhstan, state, law enforcement and special agencies work to ensure the nuclear non-proliferation regime, as well as radiation, chemical and biological safety on a permanent basis.

Considering the presence of risk factors, as well as the attempts of criminals to use their position to steal dangerous substances, including for the purpose of their sale, with a limited range of such persons and facts of criminal actions indicates a medium degree of threat of FPWMD.

The information provided in the National Risk Assessment of FPWMD indicates that, in general, the subjects of financial monitoring carrying out financial transactions take the necessary measures to counteract FPWMD:

- internal control rules are approved and followed, risk management procedures are defined, registration of suspicious financial transactions is carried out, information is transmitted to the financial monitoring body.

Subjects of financial monitoring are fulfilling all the requirements of the UN Security Council resolutions on the application of targeted financial sanctions for FPWMD.

In 2018-2020, assets and other property of persons and organizations included in the List of FPWMD in the Republic of Kazakhstan are not established.

At the same time, at the legislative level there is no need to conduct a risk assessment of FPWMD issues, identify suspicious financial transactions in this area and send reports on them to the authorized body.

Given the limited legal regulation of the issues of FPWMD in Kazakhstan, there is a risk of their use in schemes related to FPWMD.

In order to minimize the identified risk, it is required to implement a number of measures:

- in order to minimize the identified threats of FROMU, it is proposed to consider the criminalization of FROMU, in accordance with the updated FATF standards;

- improve the legislative regulation of this sphere and consider introducing special criteria developed by the authorized bodies, into the compliance procedures of financial organizations to improve the efficiency of detection of suspicious transactions possibly related to the financing of proliferation of weapons of mass destruction.