FINANCIAL SECURITY

NO. 34 JUNE 2022

P. FRADKOV:

"Public-private partnership has received a new impetus in the current environment, and this opens up additional opportunities for the implementation of infrastructure projects in Russia with the participation of small and medium-sized businesses".

CONTENTS

EDITORIAL BOARD

Chairman of Editorial Board

Yury Chikhanchin

Deputy Chairman of Editorial Board

Vladimir Ovchinnikov

Members of Editorial Board

Yury Korotkiy

Galina Bobrysheva

Vladimir Glotov

Margarita Andronova

Ivan Kornev

Oleg Krylov

Sergey Teterukov

Alexey Petrenko

German Neglyad

DEAR READERS!

We decided to dedicate this issue of "Financial Security" to the theme of partnership between the public and private sectors as well as issues of improving financial literacy of clients by national regulators and banks in order to reduce the risks of their involvement in fraudulent and other shady schemes.

The world around us is changing very rapidly and moving to new forms of interaction, mainly to the Internet environment, so today it is important to form new skills and professional competencies to effectively deal with new challenges and threats.

An important aspect is the development of partnership between the state and the private sector, which performs the tasks of primary financial monitoring and is an effective barrier on the way of illicit money flows.

The main tasks in this area are to establish a reliable mechanism of information exchange, a strong partnership between government authorities and private sector entities, as well as quality training within the anti-money laundering system.

The key to this work is coordination between all participants in the anti-money laundering system at both the national and global levels.

Yury Chikhanchin
Director of Rosfinmonitoring

COVER TOPIC - PUBLIC-PRIVATE PARTNERSHIP

PSB WILL DEVELOP PUBLIC-PRIVATE PARTNERSHIP FOR SMALL AND MEDIUM-SIZED BUSINESSES

Petr Fradkov, Chairman of "Promsvyazbank", gave an interview to the journal

Petr Fradkov

— Economic and political events in recent months have compelled many stakeholders to reconfigure their business models and change their approaches to work. How does PSB operate in the current environment?

— In fact, the Russian economy was subjected to unprecedented sanctions. Moreover, the financial sector and banks were the first to take the hit: they faced blocked foreign currency accounts of clients, outflow of funds of legal and natural persons, volatility in the financial and foreign exchange market, and a significant increase in interest rates. But thanks to the timely support measures of the Bank of Russia and the Government, the country's financial system has stabilized and is now functioning smoothly.

It is important to say that PSB had been preparing for such a scenario long before the February 2022 events. Having studied in advance the possible sanctions risks, we were able to cope with the new working conditions as quickly as possible and to protect our clients from external shocks. The February 2022 events did not have a significant impact on the bank's business and operations.

It goes without saying that the context and working conditions have changed, but life goes on, and the bank's business model has successfully passed the endurance test. Moreover, given the current situation, PSB continues to be one of the most reliable banks. We are trusted by the companies that form the backbone of the country's economy, including large, small and medium-sized businesses as well as companies that ensure the security of the State – the bank currently supports more than 70% of the defense industry contracts. Only in the first month of work under sanctions, the volume of lending to Russian companies and households amounted to 180 billion rubles.

— You just mentioned that you work with big business. What kind of support does the bank provide to Russian industry?

— As a base bank for the defense industry, PSB is steadily increasing its loan portfolio to the industry players. We work with clients from all key backbone industries such as aviation, shipbuilding, radio-electronics, etc. Let me give you an example: from February till May 2022, that is, since the imposition of sanctions, the bank's loan and guarantee support of the Russian industry has increased by 5.4% despite the difficult economic situation. Currently, we are among the leaders in lending to the domestic machine-building industry with a 40% share in the total loan portfolio of all banks. The bank is actively working on issuing preferential loans under a number of programs, including those for backbone enterprises. Amid the new conditions, we also retained our own preferential programs for the defense industry and did not revise their conditions; the average rate here starts from 4.5%.

— What are your plans for lending to retail customers and small and medium-sized businesses?

— If we are talking about the retail business, then after the reduction of the key rate there is a gradual downward trend in loan interest rates, which has already served as a good driver for the revival of the consumer finance market as a whole. At PSB, we have seen a two-fold increase in demand for loan products for the second month in a row. Moreover, under current market conditions, refinancing products are once again relevant.

We expect that the absence of new financial stresses will have a positive impact on the quality of the total consumer loan portfolio and will further increase demand for loan products by the end of this year.

In 5 months of 2022 we observe an upward trend in small and medium-sized enterprises (SME) lending: the loan and guarantee portfolio of SMEs has grown by 8% since the beginning of the year and exceeded 360 billion rubles in absolute terms. The volume of lending to SMEs in the first 5 months of 2022 exceeds by 12% the volume of lending for the same period in 2021. In absolute terms, the increase in lending in 2022 amounts to 16 billion rubles. PSB's participation in government support programs provides important support for SME lending: since the beginning of the year, within the framework of anti-crisis lending stimulation programs of the Central Bank of Russia and the SME Corporation, we have granted over 15 billion rubles in loans to SMEs and an additional 10 billion rubles – within the Interest Rate Subsidy Program of the Ministry of Economic Development (Program 1764). In total, 25 billion rubles of preferential loans. In terms of the number of preferential loans in 2022, PSB ranks second.

— The development of public-private partnership is under active discussion today. What can you say about the PSB's work in this area?

— Indeed, public-private partnership has received a new impetus in the current environment, and this opens up additional opportunities for the implementation of infrastructure projects in Russia with the participation of small and medium-sized businesses. This is a unique program of interaction between the authorities and business representatives, an exchange of necessary experience, specialists and ideas.

Most recently, on the margins of SPIEF-2022 (St. Petersburg International Economic Forum) we signed a number of agreements developing cooperation in the area of public-private partnership and concession initiatives aimed at small and medium-sized businesses. As part of joint work on such projects, PSB will provide credit facilities for their implementation.

A trilateral cooperation agreement was signed between PSB, VEB.RF and the National Center for Public-Private Partnership (PPP). We intend to develop and implement standard solutions for mass implementation of public-private partnership projects involving SMEs, including sports facilities, housing and utilities sector, pre-school education and facilities in other industries. We will offer businesses ready-made solutions for investments in infrastructure and socially important facilities with the help of PPP mechanisms.

We also signed an agreement with System Concessions LLC, under which we will build and strengthen commercial cooperation in the implementation of PPP projects. Such cooperation is aimed at increasing the number of regional private concession initiatives that develop social and industrial infrastructure in Russia.

I should also note that we have agreements on the development of PPP in the sports sector. The Bank and the Ministry of Sports are planning to promote the development of sports product manufacturing, the introduction of digital solutions and the improvement of scientific and technological activities in sports, including the use of import substitution mechanisms in the creation and modernization of infrastructure facilities and the support of sports organizations. We will also support the creation of an expert system of technological innovations in physical training and sports. Strengthening our intentions, we signed an agreement on the margins of SPIEF and we will promote the progress of domestic sports medicine, import substitution and diversification in the sports industry, as well as the implementation of sports PPP projects!

— Amid the new realities, the need to develop import substitution is obvious. How do you see the role of PSB in this process?

— In addition to financing import substitution projects for enterprises, PSB – as a bank aimed at supporting domestic industry – is a permanent platform for interaction of all stakeholders aimed at developing import substitution and diversification projects.

Among the issues that we address and discuss with the market participants are additional measures of state support for import substitution projects, issues of increasing the effective interaction of defense industry enterprises and small and medium-sized businesses in the field of import substitution, opportunities to strengthen the role of development institutions and lending institutions in organizing the financing of diversification projects and import substitution projects, promotion of scientific developments and their implementation by the project participants at the regional level, planning issues of medium-term public procurement and long-term contracts and a number of other topics.

PSB is actively involved in the development of proposals to improve measures aimed at increasing the financial sustainability of defense industry enterprises and achieving the goals of import substitution, and this work will be continued in the framework of various interagency commissions and groups, as well as expert platforms. For instance, the Bank interacts with the IDF (Industrial Development Fund) on the issues of co-financing import substitution projects. We are working on a joint initiative of the Chamber of Commerce and Industry of the Russian Federation to establish a design and engineering center with a focus on import substitution projects. I am also the Deputy Chairman of the Russian Engineering Union, supervising the Chuvash regional branch, where we promote the development of projects of industrial companies. I am a member of the Expert Council for the development of financial instruments and non-financial support measures for defense industry enterprises under the State Duma Committee on Industry and Trade, where we consider and prepare proposals on diversification as well as development of import-substituting and export production.

— Speaking of the transformation of cooperative chains, what are the primary tasks in this area?

— In the process of transformation of cooperation chains, the main problem now is making bank payments between companies. Enterprises can succeed in agreeing among themselves, even despite sanctions restrictions, but making contract payments by banks in different countries is under strict sanctions control and regulation, and it becomes a "bottle neck" for the industry. We will make a big step forward when we build our own payment system, a domestic one, but essentially an international one, to adapt to the changing cooperative chains of the industry.

When the first sanctions were imposed in 2014, the Bank of Russia began working on its own payment systems such as NPCS (National Payment Card System), FMS (Financial Messaging System) and other tools required by current circumstances. If we did not have these systems now, we would live in a completely different reality, as all payments within the country would stop. Therefore, the development of an international payment system with friendly countries and payment clearing platforms in national currencies is a priority task, if we are talking about the restoration and organization of cooperative chains. This is the area we are now focusing on, testing various options for making payments and financial transactions.

— PSB participates in the implementation of the "Sodruzhestvo" project. Can you tell us more about it?

— "Sodruzhestvo" is an international scientific and educational digital platform for working with young people who participate in the Financial Security Olympiad. The digital platform is being created with the focus on teaching the subjects of financial technology and economic security. The platform is intended to provide a unified standard of AML/CFT knowledge and become a place for the development of the talent pool in the Russian Federation and CIS member states.

We were given the task of conducting a feasibility study for the platform, as we are one of the technological leaders of the banking sector and have the necessary competencies to implement the project. In the shortest time possible, we developed a concept, conducted focus groups with students of Russian universities, as well as a comparative analysis of educational platforms operating in the country and abroad. It is planned that the digital platform will consist of five main blocks: education; interaction in the live chat format; personal account; interaction in the web lab format; job search, apprenticeships and internships. The package of documents required for the launch of the "Sodruzhestvo" project has already been prepared, which came through a successful review of the Ministry of Science and Higher Education, the Ministry of Education of Russia, Rosfinmonitoring and the Ministry of Digital Development, Communications and Mass Media of Russia.

It is estimated that the annual potential audience of the digital platform in Russia and the CIS member states will be about 3 million people. Of these, there are about 1.7 million pupils; about 1.2 million students; and about 140,000 specialists of national anti-money laundering systems.

CONTRIBUTION OF PRIVATE SECTOR TO ACHIEVEMENT OF NATIONAL AML/CFT GOALS – UNIQUE EXAMPLE OF PUBLIC-PRIVATE PARTNERSHIP

German Neglyad,
State Secretary, Deputy Director of Federal Financial Monitoring Service

German Neglyad

The year 2021 was marked by the 20th anniversary of the adoption of Federal Law No.115-FZ on Combating Legalization (Laundering) of Criminal Proceeds and Financing of Terrorism of August 7, 2021. The enactment of this legislative act marked the beginning of establishment in Russia of a robust anti-money laundering and counter-terrorist financing system consistent with the international standards – the FATF Recommendations.

The national anti-money laundering and counter-terrorist financing (AML/CFT) system of any country is inconceivable without active involvement of financial and non-financial institutions and designated private sector businesses and professions that perform critically important functions related to primary financial monitoring.

It should be emphasized that the regime of preventive measures implemented by the obliged entities is a central element of the FATF Standards and is covered by fifteen of 40 FATF Recommendations[1].

The history of public-private partnership in implementing and fulfilling the AML/CFT requirements in Russia is indicative and illustrative in this regard.

[1] FATF Recommendations 9 - 23.

While, it was important at the beginning of this process to ensure compliance by the private sector entities with the basic rules, such as arrangement of internal controls, appointment of compliance officers, identification of customers and beneficial owners and suspicious transaction reporting (which, frankly speaking, at the early stages were not always clearly understood), the AML/CFT cooperation has reached today a fundamentally new level. Despite a wide diversity of the private sector entities, cooperation with most of them, primarily with banks, is currently being developed on a basis of the shared values and common understanding of the need to protect the financial system of Russia and ensure public and economic security of the country.

In fact, the government authorities and private sector entities have become the full partners that efficiently coordinate their efforts and actively cooperate with each other for accomplishing the common goals and objectives. This is a large interrelated system incorporating over twenty government authorities and institutions and several dozens of thousands of private sector entities.

It was also highlighted by the international assessors during the mutual evaluation of Russia conducted by the FATF in 2019, who noted that domestic coordination and cooperation is one of the strong points of the Russian AML/CFT system. Besides that, good understanding of ML/TF risks and adequate fulfillment of the core obligations by financial institutions was also appreciated by the assessors.

Today, the public-private partnership is actively developing in the context of new emerging ML/TF risks. In particular, the effective cooperation mechanisms, such as the central and local compliance councils, allowed for arranging a joint monitoring of targeted spending of the funds allocated for curbing the COVID-19 pandemic. As a result of these efforts, financial institutions, primarily banks, submitted to Rosfinmonitoring eighteen thousand reports on suspicious transactions amounted in total to nearly RUR 34 billion. Based on these reports and their further analysis conducted by Rosfinmonitoring, several dozens of criminal proceedings were launched, and some of the stolen funds had been already recovered to the state budget.

At the same time, one of the specific features of the Russian AML/CFT system is that it aims to prevent criminal offences and limit the very possibility of obtaining criminal proceeds. And again, financial institutions are at the forefront of this work as they conduct thorough monitoring, scrutinize transactions and apply various measures up to refusal to carry out transactions. For example, in 2021, the private sector entities, including banks, refused to carry out RUR 122 bln worth financial transactions suspected of being related to money laundering, terrorist financing and other illegal activities. It is noteworthy, that customers typically appeal against less than 1 percent of total number of such refusals.

Furthermore, the private sector contributes greatly to the development of new financial technologies. New customer interaction forms and methods, big data analytics and other cutting-edge technologies have been introduced and are used in practice. It should be noted that the Russian financial sector is one of the most technologically advanced in the world. This is the competitive advantage that could and should be used for suppressing money laundering, terrorist financing and illicit financial transactions.

As for the prospects of further development of the partnership relations with the private sector, in our opinion, the current priorities include the following:

1. Developing common AML/CFT values and mission for the government authorities and institutions and the financial and non-financial sector entities.
2. Raising awareness of the general public of contribution of the private sector to achievement of the AML/CFT goals and enhancement of the economic and public security.
3. Promoting the AML/CFT digital transformation process, including the effective use of artificial intelligence and big data analytics for AML/CFT purposes.
4. Preventing potential diversion and misappropriation of significant amount of funds allocated currently for the support of different sectors of the economy and ensuring targeted use of these funds.
5. Improving financial literacy and enhancing financial security of public.

The potential of AML/CFT cooperation between the public and private sectors appears to remain very high, and realization of this potential will undoubtedly become a true success story of all national AML/CFT system stakeholders working for the benefit of people, society and the country.

"ANNOUNCE THE ENTIRE LIST": BANK OF RUSSIA WARNS PUBLIC ABOUT FINANCIAL PYRAMID SCHEMES, PUBLISHING THEIR NAMES ON ITS WEBSITE

Valeriy Lyakh,
Director of Department for Countering Misconduct, Bank of Russia

Valeriy Lyakh

With a view to protecting the consumer rights and promoting fair competition in the financial market, the Bank of Russia (BoR) has undertaken extensive efforts for countering the unfair practices and misconduct in the financial market, such as financial pyramid schemes, illegal lending schemes and illegal professional financial activities, over the recent years.

We conduct this work proactively by identifying illegal schemes with the use of our own monitoring system and appeals and complaints received from public. Special divisions for countering illicit activities have been created in all regional departments of the Bank of Russia, and such mechanism enables to promptly intervene and stop the spread of fraud scams in the Russia regions.

Since 2015, the Bank of Russia has identified a total of over 2.7 companies and websites indicative of financial pyramid schemes, nearly 7.5 illegal lenders, and more than 2 thousand illegal securities market dealers. Starting from June 1, 2021, the Bank of Russia publishes on its website the List of companies indicative of financial pyramid

schemes. This list contains detailed information about the companies identified since 2020, except for personal data of natural persons and individual entrepreneurs.

This List of potentially mala fide companies is updated every day based on the incoming intelligence. The main purpose of the List is to warn consumers about possible risks and to minimize potential financial losses that may be incurred by people as a result criminal activities of fraudsters. We strive to publish this information as soon as possible, because the earlier people become aware of a mala fide company, the less likely they are to be deceived by fraudsters.

At present, the List contains information about over 5 thousand identified companies suspected of being involved in illegal lending activities, illegal securities market transactions and financial pyramid schemes. This information is in high demand by the financial services users – the List page is one of the most frequently visited sections of the BoR website.

We also warn and inform public about general indicators of financial pyramid and illegal activity schemes: the most illustrative case studies and recommendations for customers are posted on the "Financial Culture" section of the website (fincult.info) and are disseminated in the BoR social media and in Telegram web.

We fight against unfair practices and misconduct in the financial market in cooperation with the law enforcement agencies and local (regional) authorities. The Bank of Russia disseminates information on all illegal schemes detected in the financial market to the General Prosecutor's Office and other competent authorities for taking the response measures.

In 2021 and in the first two months of 2022, the BoR disseminations resulted in initiation of over 140 criminal proceedings and nearly 550 administrative proceedings under different Articles of the Code of Administrative Offences of the Russian Federation, including under Article 14.56 – illegal provision of consumer loans (more than 300 proceedings were launched under this Article). Besides that, over 4.7 thousands of other response measures were taken[1], which included termination of website maintenance agreements and restriction of access to over 3 thousand websites of illegal financial market participants and pyramid scheme operators. These performance indicators are good enough, showing that cooperation has been excellently arranged at both federal and regional levels. In our opinion, further integration and more active involvement of the Bank of Russia in the national anti-fraud efforts may become one of the consumer protection priorities at this stage.

The use of the capabilities of the "Know Your Customer" platform will become a new stage in the fight against companies suspected of being involved in illegal activities and financial pyramid schemes. This platform is a special information service that will allow banks to obtain information on risk of potential involvement of their customers (legal entities and individual entrepreneurs) in suspicious transactions. All customers will be subdivided into three groups depending on risk level: high, medium and low. We also plan to add data from the List to the "Know Your Customer" information platform. This will enable a seamless integration of information about risks into the compliance procedures of credit institutions. As regards other entities suspected of being involved in illegal activities in the financial market (without registration with the tax authorities), updated information for implementation of a range of AML measures provided for in the internal control rules will be disseminated to credit institutions via the Personal Account so that they can take adequate response measures proportionate to risks. At present, different ways of implementation of these plans are being discussed.

Unfortunately, the 2021 has demonstrated that new technologies can be successfully exploited by fraudsters and can help to invent illegal schemes in a more simple and cost-effective way. In particular, the opportunities provided by the social networks multiplied the audience engaged in illegal schemes and made the fraudulent advertising campaigns more targeted and efficient. At the same time, anonymity intrinsic to modern communication instruments

[1] Termination of website maintenance agreements, restriction of access to websites, orders to eliminate breaches of the legislation, applications to courts for changing the names, prohibition of operations, etc.

makes it more difficult to identify the masterminds of fraud schemes and scams. To address these challenges we use the provisions of the new law adopted last year that authorizes the Bank of Russia to block websites without obtaining court order. By now, over 600 pages in the Classmates and InContact social media and 8 Telegram web channels have been blocked in this way.

No matter how quickly suspicious websites are blocked, we understand that this will not resolve the problem as fraudsters may easily create the "mirrors" of the blocked websites and quickly launch new "projects" and associated websites. At present, the investment topics are actively exploited by almost all financial and pseudo-financial bloggers and by the majority of websites indicative of financial pyramid schemes. They use various advertising opportunities and offer exotic investment proposals ranging from offering non-existing cryptocurrences to obviously fake proposals. However, it is impossible to prohibit such advertising activities as no restrictions for attracting investments are currently provided for in the applicable legislation.

In our opinion, prohibition of attracting investments from public by companies that are not supervised by the Bank of Russia may help to partially address this problem, and the Bank of Russia has already initiated the discussion of necessary amendments to the legislation. In particular, it is proposed to update the existing definition of "investments", and to specify that investments mean funds or other assets placed for making a profit for investor. We also propose to prohibit consumer associations from raising loans from other parties other than their members.

However, it is obvious that that such legislative initiatives only complement the existing mechanisms of cooperation with the law enforcement and other competent authorities and domain name registers in the fight against illegal companies and financial pyramid schemes.

DIGITALIZATION AS A DRIVER FOR ENHANCING FINANCIAL LITERACY

Mikhail Mamuta,
Head of the Service for Consumer Protection and Financial Inclusion at the Bank of Russia

Mikhail Mamuta

Russia is one of the world leaders in the digitalization of financial sector. So, the share of cashless payments in our country exceeded 75%; over 90% of bank accounts are managed on a remote basis; and 12.9 million people consented to use a digital profile.

At the same time the need to sharpen financial service customers' skill set in using digital services and remote channels is getting more and more urgent, meaning that new risks and challenges in the work of enhancement of digital financial literacy are emerging.

In the first place, it is digital skills inequality, including with respect to basic knowledge and hands-on experience in utilizing digital financial services, especially among people of older age. Next, these are new fraud schemes, specifically, those involving social engineering. Finally, it is the distribution of complex combined financial products and the employment of mala fide practices by market players (e.g. misselling).

It sets the requirement for further protection framework of retail investors and consumer rights and for integrated systematic efforts to enhance investment, digital and cyber literacy. These areas are mapped out in the Public Financial Literacy Strategy to be completed in 2023. In implementing the Strategy, the Bank of Russia in close cooperation with the Government of the Russian Federation utilizes all potential tools and channels.

As far as school kids and youth in general are concerned, the primary focus here is integration of financial literacy into the education system. In 2021, new FSES (Federal State Educational Standards) developed by the Bank of Russia together with the Ministry of Education to include financial literacy were approved for the elementary and high school. In the elementary school it will feature in such subjects as 'Mathematics' and 'Environment' and in grades 5–9 – in 'Social Science', 'Mathematics' and 'Geography'. New standards training will start as early as on September 1 this year. For instance, 1–4 grade pupils will be able to acquire Internet safety skills, including during financial transactions. While 5–9 grade pupils will learn how to assess business risks, as well as about bad practices resorted to by financial entities and various financial fraud schemes.

Also, since 2015 pupils, college students and those raised in orphanages and children's homes at any location across Russia can attend online financial literacy classes conducted by employees of the Bank of Russia and leading financial institutions. Experts instruct students how to safely use bank cards and to identify Internet frauds and answer other questions that any person might have when managing his or her finances through digital channels. In 2021, about 25,000 schools joined the project with classes getting over 4.76 million views. This year, the spring sessions of online classes have gained over 2.5 million views.

Training and information providing work is conducted by the Bank of Russia outside the scope of the educational process as well. In this work, digital channels provide the most user-friendly and accessible formats for each target audience. These include social media and popular websites and interface with bloggers. Videos containing financial literacy topics are shown at train stations, airports and subways. Leaflets and booklets are available at MCPS's (multifunctional centers for public services) and post offices. Significant portion of these materials is dedicated to cyber safety, enabling people to identify online frauds and avoid becoming victims of their tricks. Considering that criminals regularly come up with new fraud schemes, the information awareness process goes on non-stop: The Bank of Russia updates its materials, provides information on new schemes and strongly recommends to people to be on the alert when it comes to money.

One of the enhanced financial literacy formats gaining momentum from year to year is the annual All-Russia financial online test. Each year the number of those who wish to check their financial literacy proficiency gets higher, and in 2021 above 600,000 people — from pupils to pensioners – took part in it. The test includes digital financial literacy questions, specifically, remote finance control, data protection, countering methods of social engineering and many other aspects. The test allows not only checking but building up financial knowledge — if the participant gives a wrong answer he or she is provided with relevant explanation and a link to a useful material. Also, data obtained during the test helps the Bank of Russia determine the financial literacy level across the region.

The Bank of Russia 'Financial Culture' website plays an important role in the public awareness campaign. At this site people find answers to their questions on financial subjects without hidden offers of any products or services, or promotions of specific financial entities. The key advantage of the website is that materials are delivered in simple and understandable format. Here you can come across the updated list of fraud schemes entitled 'Traps' you'd better not fall into. In addition, the regulator makes a wide use of Yandex services, i.e. Yandex.Zen and Yandex.Q through which the fincult.info editorial board answers users' questions relating to finance. The Bank of Russia has created and is actively developing the 'CB-Online' mobile application that enables the user to put questions to the regulator. Application users can also verify the legality of a financial entity and read through useful publication on the financial subject.

The online access to the stock exchange market and options of opening a broker account at the push of a single button, as well as of making an investment

from any location across the globe tend to make the securities market most attractive to the Russian people. A massive inflow of inexperienced unqualified investors was spotted in the market in 2020 and in early 2021. Those are people who lack necessary knowledge and experience, but wish to enlarge their savings, and most commonly search for useful information to accomplish that on the Web where there are plenty of relevant tips and pointers, and it is very difficult to sort them out. Investors frequently encounter unscrupulous consultants and substandard programs offered by some market players whose intent is only on selling their product or intermediary services. The Bank of Russia gets pro-actively involved in this process aiming to give people appropriate guidance on searching for learning programs, to grant access to high-quality knowledge and to exclude anything that may be related to fraudulent activities. In this context, it should be noted that the Financial Literacy Association hosted the developed accreditation system for financial literacy enhancement programs.

Furthermore, the Bank of Russia is active on two fronts at the same time, i.e. public awareness of financial issues and protection of financial service customer rights. The regulator lays out requirements for financial entities to keep their clients informed, assess their knowledge and understanding of special features and risks inherent to products acquired, recommends to a company relevant business models and where necessary responds to customer complaints. Protection measures against fraud schemes, including those available in the Internet, are built up by the financial regulator in close collaboration with law enforcement authorities.

The Bank of Russia pays special attention to protecting the most vulnerable social groups. In order to make financial services not only more accessible, but secure to disabled and old aged persons, in 2021, the Bank of Russia formulated recommendations for banks according to which such client may deactivate remote access to his or her account thus diminishing the risk of becoming a victim of fraud or social engineering. According to the regulator's monitoring data, over 60% of banks have either brought into effect these recommendations or are in the process of developing relevant implementation algorithms. Also, banks are advised to put into place a ‘second hand’ service when a person may on an arrangement with another client of the same bank (e.g. his or her relative) appoint him or her his or her assistant who will additionally be in charge of money transfer transactions and authorized to block them if he or she deems them to be suspicious. A similar service is already in operation at one of the largest banks in Russia.

It is obvious that new digitalization challenges to the financial world require a comprehensive approach to be taken, i.e. financial information awareness, protection of consumer rights and working with financial institutions to reshape the client servicing culture. For a desired outcome to be achieved, a concerted effort of interested parties is required, i.e. by federal and regional authorities, the Bank of Russia, public entities, the Financial Literacy Development Association, foundations and volunteers. Only in this case the digital transition will make the access to financial services really up-to-date, convenient and safe.

PUBLIC-PRIVATE PARTNERSHIP AS A FOUNDATION OF THE ANTI-MONEY LAUNDERING SYSTEM. RELEVANT ISSUES OF THE INTERACTION BETWEEN THE PRIVATE SECTOR AND GOVERNMENT AUTHORITIES IN THE NATIONAL AML/CFT SYSTEM

Financial security is the basis of economic development of any nation and the most vital component of safety of any person and the public as a whole

Elena Smirnova,
Special officer at "Praktika LK" LLC

Elena Smirnova

Financial security in Russia is becoming especially relevant under unprecedented economic pressure on the part of unfriendly countries. In the current situation, anti-money laundering (preventing the legalization of illegal proceeds) and even more so countering terrorist financing are of vital importance for maintaining a sustainable development pace for our country's economic development.

The foundation of the Russian anti-money laundering system is constituted by entities that provide financial services and perform monetary and property transactions. The overall performance depends on the extent to which these entities are involved and on how much they are engaged in the system; it is these entities that should be in the first place aware of the transparency of each transaction and deal and assess the exposure of clients to the risks of participation in shadowy or illegal business activities. In order to pursue these goals,

entities apply customer due diligence and business operations analysis techniques, determine origin of funds, and monitor operations. In case of high risks being identified, they would be in a position to refuse to close a deal or perform a transaction for the client. Furthermore, all cases of suspicious activities and dubious transactions are properly reported by entities to Rosfinmonitoring.

Therefore, further development of the national AML/CFT system is directly related to the level of interaction between government authorities and the private sector. For the time being, actions taken by Rosfinmonitoring in the leasing sector demonstrate high effectiveness: the level of compliance in the sector has reached 78%; leasing companies submit information on screening the names of their clients against the Lists; they actively submit information on transactions subject to mandatory control; suspicious transactions reporting also remains on a fairly high level. The sector of leasing companies is well informed about potential involvement into illegal activities and ML/TF risks and takes appropriate countermeasures.

One of the most required tools of AML/CFT interaction and feedback, specifically, with external restrictions in place, is the Personal Account on the Rosfinmonitoring website that also operates as a web portal for reporting mandatory and suspicious transactions; a feedback channel; and a digitalization component for supervision activities. The Personal Account can be used as a conduit for remote education, i.e. it hosts video courses of most relevant topics of entities' participation in the AML/CFT system and a testing system is deployed.

One of the primary issues Rosfinmonitoring needs to address is making new preventive arrangements for reducing ML/TF risks and countering the inflow of criminal proceeds into legal business turnover. Information sharing on emerging risks with private sector representatives and forwarding identified typologies are normally done by the Compliance Council. This advisory body ensures functioning of efficient feedback framework, develops criteria and financial behavior models relating to criminals with a view to enhancing efficient and prompt ways of uncovering transactions associated with respective risks.

Also, Rosfinmonitoring consistently pays great attention to providing training courses and guidance on legal compliance in the AML/CFT area. Active interaction has been organized with the professional community, i.e. the Unified Leasing Association.

Also, Rosfinmonitoring makes an extensive use of conducting questionnaire surveys of supervised sectors on relevant issues. Obtained findings and proposals are taken into account in the regulator's activities. For example, targeted surveying results were used to prepare a final report on ML/TF sectoral risk assessment.

Currently, Russia has in place and operates a system, which provides integrated implementation of and compliance with the AML/CFT laws. However new threats to economic safety (primarily, economic sanctions) and innovations in Russian economy (import substitution, digitalization, etc.) set a requirement for ongoing efforts to further advance AML/CFT methods and practices and develop the public-private partnership, including:

- improving information support to AML/CFT sub-systems and levels;
- expanding interaction platforms to share experience and information and upgrade the professional expertise of AML/CFT subjects;
- building up digital compliance systems that will be adjusted by means of automation depending on variations in the conduct models employed by criminals;
- adjustment of the Personal Account for ongoing conduct of remote events and exercising preventive measures.

PUBLIC-PRIVATE PARTNERSHIP AS A FOUNDATION OF THE ANTI-MONEY LAUNDERING SYSTEM

As demonstrated by the interaction between the Ministry of Taxes and Duties of the Republic of Belarus and gambling organizers

Marina Nevinskaya,
Head of the Gambling Business Department, the Ministry of Taxes and Duties, the Republic of Belarus

Marina Nevinskaya

In effect from April 4, 2012, gambling organizers in the Republic of Belarus will be classified as entities performing financial transactions, while the Ministry of Taxes and Duties (hereinafter in this article - the 'Ministry') has been designated as an authority supervising their activities, including control over compliance by such business entities with applicable AML/CFT laws[1]. Currently, the legal framework for this decision is provided in Law of the Republic of Belarus No. 165-Z dated June 30, 2014 'On Measures for Anti-Money Laundering, Countering Terrorist Financing and Countering Proliferation of Weapons of Mass Destruction'.

For reference:
As of April 1, 2022, gambling licenses are issued to 119 legal entities.

Today the main prerequisite for gambling business operations in Belarus is the connection of gambling equipment and offline & online gambling establishments to a dedicated computer cash system providing control

[1] AML/CFT stands for Anti Money Laundering and Countering the Financing of Terrorism.

over gambling business turnover (the 'special system') based on the public-private partnership functioning in the Republic from December 1, 2013.

The key purpose behind creating this special system is placing under effective control the gambling business. One of the underlying principles of this control is providing continuous monitoring of implementation by gambling establishments, including online casinos, of legislative requirements. The processes of such governmental control involve gambling organizers, competent government authorities and the monitoring center that are components of the special system.

Currently, with the special system's features being used, special forms are submitted to the financial monitoring authority by gambling organizers, visitors are identified and high-risk clients, including PEPs, are authenticated; the special system incorporates black and gray lists of the FATF and national lists of terrorists and offshore jurisdictions, and provides reporting framework for gambling subjects to set up and operate effective internal controls in their respective offline and online gambling establishments.

To ensure 24/7 operation of the special system, the monitoring center that provides to gambling organizers technical support as well as information guidance on the application of the AML/CFT legislation was established. Quarterly, more than 50 representatives of gambling organizers contact the monitoring center for clarifications of provisions of the AML/CFT legislation.

Workshops and round-table meetings regularly organized by the ministry, the monitoring center, involving representatives from private business and government authorities, including the National Bank of the Republic of Belarus and the Financial Monitoring Department at the State Control Committee of the Republic of Belarus, play a vital role in building up the public-private partnership with gambling business entities.

In order to raise the awareness of the gambling organizers on legal issues of risk management related to money laundering, terrorist financing and financing of proliferation of weapons of mass destruction (the 'risk management'), tax authorities provide information guidance to gambling organizers on relevant risk management recommendations formulated by the Ministry using the special system's functional features. Therefore, understanding the importance of the public-private partnership as the long-term cooperation model of government authorities and business allowing an effective nationwide anti-money laundering system to be developed, the Ministry focuses its attention both on maintaining direct interaction with supervised gambling subjects regarding AML/CFT issues and on leveraging the potential of the monitoring center and the special system.

PROSPECTS OF THE PUBLIC-PRIVATE PARTNERSHIP IN GENERATING AND ANALYZING BENEFICIARY OWNERSHIP INFORMATION

Soat Rasulov,
Administrator of the EAG Secretariat

Soat Rasulov

One of the most commonly known legendary biographies says that the 19th century famous banker Nathan Rothschild earned his fortune because he was the first to get information about the outcome of the battle between forces led by Napoleon Bonaparte and British general Arthur Wellington. Hence the following expression is ascribed to him: 'He who owns information, owns the world'[1].

Naturally, verified information does not only allow handling financial matters, but also helps to promote public interests. Where such information is in the public domain it may prevent or reveal anti-social events.

It is the openness and transparency of information that the standards of the Financial Action Task Force (the FATF Recommendations[2]) are focused on, requiring jurisdictions to maintain trade and commercial registers open to the public, lists of registered corporations and companies, and lists of commercial and trading permits.

[1] https://steemit.com/steemit/@sergrom/who-owns-the-information-he-owns-the-world-who-said-this-phrase.

[2] Documents - Financial Action Task Force (FATF) (fatf-gafi.org).

Specifically, the FATF Recommendation 24 requires countries 'to adopt measures to prevent misuse of legal persons for money laundering or terrorist financing', including mechanisms determining 'processes for obtaining and recording general information and beneficiary ownership data and making the aforementioned information publicly accessible'.

Today the practice of maintaining public trade registers containing general information on registered legal entities is implemented in nearly all countries around the globe. Access to some registers is free and unlimited, while access to others is granted for a fee. There are also incorporated companies information aggregators disclosing data on a contract basis.

It is evident that one portion of requirements for registers is implemented rather effectively, while the beneficiary ownership information collection process requires fundamental improvement. According to the FATF analysis[3], about 9 percent of nations around the world that have undergone mutual evaluations have been able to efficiently implement standards relating to prevention of misuse of legal persons for money laundering and terrorist financing.

However, the top performers are those jurisdictions that have used a multi-pronged approach to beneficiary ownership information collection. Such an approach implies concurrent use of several sources showing who ultimately owns, manages or benefits from the company's business.

40% of countries refer to information collected by financial/non-financial entities, trade registers and legal entities themselves as the source of beneficiary ownership data. A slightly smaller portion (38%) makes reference to the first two sources of information. 19 percent make use of data available to legal persons and financial/non-financial entities.

In the context of the information provided above, it might be interesting to explore what expertise the Republic of Uzbekistan has to share regarding integrated data collection. It should be noted that at the time this article is written, Uzbekistan has yet to complete the mutual evaluation procedure.

If you refer to public sources, you may find out that for the last 5 years, Uzbekistan has been consistently rising in the international rankings on business openness and investment climate improvement. One of the essential measures in this direction has become adoption of a new approach to registering legal persons.

Resolution of the Cabinet of Ministers of the Republic of Uzbekistan No. 66[4] dated February 9, 2017 approved the state registration procedure for business entities substantially simplifying the document assembly and submission procedure for formalizing the legal establishment of business. In parallel, this resolution updated the Unified State Register for Business Entities (USRBE), its data sources and structure and openness requirements for external users.

In December 2020, certain changes were made to the application form for legal entity incorporation according to which beneficiary ownership information pertinent to a newly created legal entity should always be filed when approaching the registrar. However the procedure relying on the good-faith conduct of applicants provided no guarantee of the truthfulness of received information, nor the registrar had any adequate resources to verify it.

The emerging requirement to verify beneficiary ownership gave rise to selecting other options for validating its veracity. A choice was made in favor of the data collected and analyzed by commercial bank under the framework of customer due diligence (CDD) programs.

In Uzbekistan, settlements in cash between legal entities are prohibited with the legislation permitting them to use only bank accounts that may be opened only by commercial banks licensed by the Central Bank. In their turn banks are bound to exercise preventive measures for countering money laundering and terrorist financing, including verification of beneficiary owners[5]. In the course of verification, banks accumulated updated and reliable data on beneficial owners of all companies in the country.

[3] http://www.fatf-gafi.org/media/fatf/documents/recommendations/Report-on-the-State-of-Effectiveness-Compliance-with-FATF-Standards.pdf.

[4] https://lex.uz/docs/3111342.

[5] https://lex.uz/docs/3212192.

In the process of collating accumulated data with relevant details in the state register the public-private partnership principle was applied. Banks were offered to check the information kept in the USRBE against their own beneficiary ownership data and if any discrepancies are found, to indicate them. The Central Bank consolidated the information and submitted it to the Ministry of Justice responsible for maintaining the register and the State Tax Committee. As a result, the found discrepancies, including those pertaining to beneficiary owners, were corrected by legal entities according to requirements of tax authorities by submitting relevant applications to the registrar within justice authorities structure.

Such a framework has both strengths and weaknesses. The main advantage is providing updated and verified data on beneficiary ownership in the single register along with general information on legal entities. The downside is an additional supervision function vested in the bank that, nevertheless, is compensated by perspective of reduced verification efforts due to concurrent use of administrative resources available to government authorities.

Also, the employment of this framework requires extremely cautious and sound approach from a perspective of compliance with the banking secrecy laws. For example, the Law of the Republic of Uzbekistan No. 530-II[6] dated August 30, 2003 'On Banking Secrecy' does not treat beneficiary ownership information as either a portion of customer data, or an independently guarded secret, which simplifies data exchange between banks and government structures.

Uzbekistan has yet to come a long way towards improving techniques for identifying and verifying beneficiary ownership information. In an environment where criminals apply any method of concealing illegal and legalized proceeds, the range of sources of information used to update the USRBE is insufficient. However, we are already past the starting point and one of the prospective mechanisms of upgrading the quality of collected data is already employed by the government regulators with support of the private sector.

Finally, it should be noted that compilation process of the unified register containing not only general information but also beneficiary ownership data is becoming mandatory as a result of revision of Recommendations 24 by the FATF in March 2022.

[6] https://lex.uz/docs/41882.

KAZAKHSTAN'S EXPERIENCE OF INTERACTION BETWEEN FINANCIAL INTELLIGENCE UNIT AND THE PRIVATE SECTOR

Timur Musin,
Compliance and AML/CFT Expert (Republic of Kazakhstan)

Timur Musin

The private sector represented by primary financial monitoring subjects is an essential component in the national AML/CFT system taking action to reduce risks, including in the process of identifying suspicious clients and their transactions. The involvement of primary financial monitoring subjects in anti-money laundering and terrorist financing (the AML/CFT) processes and the level of information awareness of mandatory requirements and understanding of ML/TF risks have a direct effect on the quality of information obtained and used by a financial intelligence unit in preventing money laundering and terrorist financing.

That is why maintaining efficient liaison between government authorities and the private sector and building up continuous communications and feedback channels are vitally important in the AML/CFT national system. Generally, the AML/CFT development concept, from our perspective, should rest on the following priorities:

- enhanced analytics quality;
- continuous improvement of AML/CFT processes;
- enhanced preventive role of a financial intelligence unit (FIU);
- ensuring inevitable responsibility

Recent years witnessed the building up of a system of continuous interaction between the financial intelligence unit - the Financial Monitoring Agency of the Republic of Kazakhstan with financial monitoring subjects, which has resulted in the qualitative growth of information submitted by the private sector to the financial intelligence unit compared to previous periods.

It should be noted that in addition to existing official communication channels, the interaction between the financial intelligence unit and financial monitoring subjects is provided by the compliance council acting as a discussion platform where representatives of the financial intelligence unit and other government authorities and also representatives of financial monitoring subjects can share views and practices and coordinate their efforts in the AML/CFT process. Specifically, this compliance council allows discussing:

- relevant cases as part of joint efforts;
- problematic issues or potential changes to laws and regulations;
- initiatives put forward by the financial intelligence unit and also to receive proposals from financial monitoring subjects

Similar meetings are conducted both by the financial intelligence unit and its regional offices. From my personal experience, I can make reference to the active collaboration with the Almaty Economic Investigation Department that, following continuous work on countering illegal cashing-out, expressed gratitude to a number of financial monitoring subjects for their input in the fight against the shadow economy, including myself. These joint activities raise the level of mutual trust.

The key to success in creating an efficient AML/CFT system is also promoting the AML/CFT culture in the framework of which a correct behavior model for government officials and representatives of financial monitoring entities is developed. In this case the AML/CFT requirements are perceived as a duty to the country and the public to efficiently enforce the financial security policy rather than the formal requirements of the legislative system or of internal documents of financial monitoring subjects, which ultimately has a positive effect on the financial market, economy as a whole and the quality of life of people. Well, it is the most important matter in any such initiatives.

This is why creating fair and square processes in financial monitoring subjects to identify existing shortcomings and breaches is always better than any situations where, on the contrary, processes are concealed presenting a sort of decoration which in reality hides a miserable plight. Further development of similar processes and the implementation of the risk-based approach will enable financial monitoring subjects to act more efficiently without any apprehension that they could be punished for open transformations in contrast to those who tend to operate in a different manner. It is vitally important not to discourage the private sector from this positive practice, otherwise the effect could be reversed, unfortunately.

Another essential component required for efficient AML/CFT processes is the inflow of new experts to the financial intelligence unit. Specifically, in recent years the FIU on the regular basis selects candidates from a pool of students or young professionals of private sector who could enrich the work with something new or innovative. I have a reason to believe that further mutual supplement of personnel is a positive trend and will facilitate:

- the financial intelligence unit to bring in employees in different spheres (e.g. the securities market, digital assets, payment institutions, etc.);
- the private sector to attract experts from government authorities that will be able to introduce high AML/CFT standards and new approaches to an entity's activities.

Private sector personnel development is also a factor to be reckoned with. If previously a regulation laying out AML/CFT education and training requirements for financial monitoring subjects made it necessary to train an entity's personnel on certain programs, currently there are no such restrictions in place, which give financial monitoring subjects an extensive range of options in the process of selecting or developing training material for their personnel. At the same time, the requirements for assessment of acquired knowledge have been toughened because of the added rule of undergoing regular tests at the National Center for Civil Service Personnel Management.

The value of personnel training on AML/CFT issues can hardly be overstated since the formation of the anti-money laundering culture is an ongoing process and it means more than one-time development of an

AML/CFT internal document matched by one-time familiarizing with the requirements it contains.

There are currently in Kazakhstan a number of AML/CFT certification and compliance programs that are available to a broad scope of financial monitoring subjects. It can be illustrated by the following examples:

- the AML/CFT certification program at the Association of Financiers of Kazakhstan;
- AML/CFT certification and compliance program at the Astana International Financial Center (the AIFC)

If one program is devised to upgrade the qualifications of personnel of financial monitoring subjects represented by financial institutions (banks, insurance companies, and professional players at the securities market), the other one is focused on AIFC members with the bulk of them being from fin-tech firms.

Speaking of the AML/CFT culture development we should bear in mind other activities that are carried out on an ongoing basis by the financial intelligence unit, the private sector and other government authorities. Here the following aspects should be highlighted:

- prevention of cashing-out operations where major financial monitoring subjects such as banks operating on the second level have become a powerful tool for reducing the volume of cashing-out;
- regular development by the financial intelligence unit of typologies that help financial monitoring subjects more efficiently reveal criminal schemes;
- formalization of requirements regarding digital assets and also customer due diligence processes related to such high-risk assets;
- expansion of the list of financial monitoring subjects by including AIFC members undertaking individual activities to issue digital assets, arrange for auctions of those assets and also to provide services of exchanging digital assets for money, valuables and other property; and formalization of new scenarios of suspicious transactions that apply to yet unaffected areas;
- enhancement of the AML/CFT law with provisions related to politically exposed persons and maintaining list of such persons

Generally speaking, I am confident that the development and maintenance of efficient interaction between the financial intelligence unit and financial monitoring subjects should continue contributing to raising effectiveness of the AML/CFT system in the Republic of Kazakhstan.

PUBLIC-PRIVATE PARTNERSHIP AS A FOUNDATION OF THE ANTI-MONEY LAUNDERING SYSTEM

Ardak Mukasheva,
Managing Director/Chief Compliance Controller of Jusan Bank JSC (Kazakhstan)

Ardak Mukasheva

In order to describe the practice of interacting with competent government authorities in the AML/CFT sphere, I had to recollect what happened thirteen years ago: we together with our colleagues from the banking community and the then Financial Monitoring Committee (FMC) were discussing the first legislative requirements of the Republic of Kazakhstan in the anti-money laundering field.

It should be acknowledged that neither we, nor our FMC colleagues could, to the full extent, realize how the main international and national financial monitoring requirements were to be met without negatively affecting the overall business development strategy.

But our collective brainstorm and joint efforts, and, I would say, our enthusiasm had produced positive results both in the operation of the private sector and the entire national AML/CFT system.

Certainly following each such victory new tasks were set to improve internal control processes, to conduct customer due diligence according to international standards and to develop financial monitoring procedures.

What picture can we see today?

The public-private partnership (PPP) concept of the Republic of Kazakhstan has been arousing a lot of interest around the world for ten years now. The process of building up the anti-money laundering system and interaction between the private sector and government authorities has acquired a clear strategy built into this concept.

As was remarked by Marek Belka, the Executive Secretary of the United Nations Economic Commission for Europe "…PPP combine the best of "two worlds": the private sector with its resources, management skills and technology; and the public sector with its regulatory action and protection of the public interests. This balanced approach is especially welcomed in the delivery of public services which relate to every human being's basic needs."

According to the main provisions of the Practical Guidebook developed by the UNECE for politicians, government servants and representatives of the private sector, in order to obtain positive results from the PPP functioning, it is necessary: to develop institutions; observe transparent and efficient procedures for implementing projects; hold authorities accountable to the public; and have in place competent government and private sectors, i.e. 'efficient management'. This guidebook incorporates the main principles of PPP management:

1. Participation: the level of involvement of all stakeholders;
2. Decency: the extent of rule creation and compliance control without causing any damage or discontent;
3. Transparency: the clarity and openness of the decision-making process;
4. Accountability: the degree of responsibility to the public for everything said or done.
5. Fairness: the extent to which the requirement to follow and abide by the rules equally applies to all members of the public.
6. Efficiency: the utilization rate of limited human and financial resources without losses, delays or damages or causing no harm to the next generations.

In the light of the above, acting as a member of the overall AML/CFT system in the Republic of Kazakhstan, banks comply with established provisions of normative legal acts in the AML/CFT field primarily provided in the existing Internal Control Rules (the 'Rules') of each financial monitoring subjects (FMS) developed considering all inherent client risks and risks of using services for criminal purposes, including the risk of misusing advanced financial technologies. It should be noted that representatives of the private sector in cooperation with competent authorities (FMA (Financial Monitoring Agency), FMRDA (Financial Market Regulation and Development Agency), NBRK (National Bank of the Republic of Kazakhstan), etc.) play an active role in elaborating the legislation with due consideration to the existing legal practice.

Banks are continuously improving in-house AML/CFT measures, i.e. due diligence processes, efforts to identify suspicious transactions, measures to mitigate the risk of using bank services for committing or assisting in ML/TF offences that would negatively affect bank's reputation.

One of the most important components of the efficient AML/CFT effort is the targeted, timely and high-quality training of personnel of primary financial monitoring subjects on legislation compliance and internal bank rules. So, regular training and knowledge assessment of personnel on AML/CFT issues are provided under the framework of the personnel training and educational program both as part of full-time and remote training; also, to provide skill development training of personnel at dedicated AML/CFT business units, such personnel is actively enrolled in workshops, training sessions and other educational/training programs conducted by external organizations engaged in AML/CFT training. Here FMSs use materials, experience and knowledge of experts of competent government authorities in the Republic of Kazakhstan and international organizations thus facilitating experience and knowledge sharing in such a vital area as countering ML/TF.

One of the most important components in the AML/CFT system is the process of financial monitoring and identifying indicators of suspicion both in FMS client transactions and behavior of clients themselves. Identification of indicators of suspicious transactions may set off analysis and in-depth inquiry into such transactions. Normally, going

beyond the criteria specified in applicable bank in-house regulations relating to the AML/CFT field, a FMS takes into account other internal and external factors that, in its turn, get prioritized according to the effect on the transaction/client assessment.

Drawing on the judgment made in the course of analysis of client transactions, client activities, and client information obtained from various sources, including personally from a client, financial monitoring subjects independently decide whether to qualify a transaction as suspicious or not.

Identifying client transactions, a client and his/her activities as suspicious is closely interconnected with the work of analytical center of a competent AML/CFT authority. The process of identifying and mechanism of information sharing on suspicious transactions is a long-standing and field-proven practice of FMS interaction with competent AML/CFT government authorities already provided for in respective regulations of the Republic of Kazakhstan.

We also understand that it is a bank itself that can have the most efficient means of managing the risk of bank involvement in suspicious transactions, including taking independent decisions on blocking or refusing to carry out a transaction. This process also runs flawlessly and is well organized in many FMSs.

The investigation process includes submitting information requests and respective documents from clients for purposes of exploring economic justification and purpose of carrying out a transaction. Ultimately, the investigation culminates in formulating a conclusion of whether or not the client or client's transactions are suspicious which is followed by taking restrictive measures. The quality of financial investigation at the FMS level impacts the extent of law enforcement measures to be taken.

It should be noted that the analysis brings to light the following statistics: requests and inquiries from law enforcement authorities are forwarded for the most part (over 80%) regarding persons who have earlier been reported by FMSs to the competent authority, which indicates that these requests and inquiries are forwarded in response to measures taken by FMSs.

All above mentioned is the result of work of efficient competent business units set up within FMSs, commonly, the Compliance Control Department employing personnel with sufficient experience in AML/CFT and compliance, and, normally, they are all certified and have repeatedly received awards and diplomas.

At the same time it should be noted that the AML/CFT internal control system should be focused on preventing money laundering and terrorist financing, i.e. by FMSs providing comprehensive financial monitoring of client transactions and efficient use of information systems and software designed to detect suspicious transactions before their completion to reduce bank exposure to legal risks, including money laundering and terrorist financing risks.

At every stage, where the bank acts as a controlling unit, for example, as a currency control agent or as a financial monitoring subject, all processes are aligned based on specifics of certain legal requirements and internal bank processes. If any changes are introduced (regardless whether in the bank or in the legislation), each change is discussed both with the market and competent government authorities in the Republic of Kazakhstan. There is practice of analyzing recommendations of international organizations, global banks and auditing firms.

In conclusion, it should be noted that the AML/CFT system in the Republic of Kazakhstan is still developing and we, specifically, representatives of the private sector, and FMSs staff are ready to actively participate in the process. So, for example, an active group of FMSs employees is already participating in working groups at Majilis in the Republic of Kazakhstan, interagency working groups and working groups at the FMRDA, International Compliance Council set up under the auspices of the EAG, which has a positive effect on the efficient functioning of the AML/CFT national system. Also, such interaction highlights mutually beneficial cooperation between the private sector represented by FMSs and competent government authorities.

Along with what has been said below, FMSs are ready to discuss proposals to enhance monitoring

procedures both at their level and at the level of competent government authorities:

- regarding enhanced control to make sure that turnover corresponds to the real capacity of a specific entity engaged in foreign economic activities, transaction details and other evaluation criteria;
- a possibility of putting in place restrictive measures when indicators of suspicion regarding smuggling, illicit imports/exports and other suspicious transactions are identified;
- the scale of business operations matches both the profits stated by business entrepreneurs and the cross-border turnover performed by them across the border of the Republic of Kazakhstan.

Therefore, consolidated involvement in the monitoring process not only of the financial sector participants, but also respective government competent authorities will result in integrated risk-based approach in the AML/CFT system of the Republic of Kazakhstan.

The ultimate goal is not to miss achieved opportunities but improve and develop communication and interaction mechanisms between all participants in the AML/CFT system of the Republic of Kazakhstan.

ON THE IMPLEMENTATION OF MEASURES AIMED AT PREVENTING MONEY LAUNDERING IN THE NOTARY PRACTICE OF THE REPUBLIC OF BELARUS

Olga Ryzhankova,
Notary of the Minsk City Notary District (the Republic of Belarus)

Olga Ryzhankova

The Constitution of the Republic of Belarus, the Law of the Republic of Belarus of 30.06.2014 No. 165-Z "On measures to prevent the legalization of proceeds from crime, the financing of terrorist activities and the financing of the proliferation of weapons of mass destruction" (hereinafter — Law No. 165-Z), other legislative acts, as well as international treaties of the Republic of Belarus constitute the legal basis for the activities to prevent the legalization of proceeds from crime, the financing of terrorist activities and the financing of the proliferation of weapons of mass destruction.

According to the second part of Article 1 of Law No. 165-Z, persons engaging in financial transactions, for the purposes of this law, also include notaries.

In notarial practice, difficulties arise when notaries identify the beneficial owners of their clients in the following cases:

- in relation to closed joint stock companies and open joint stock companies in cases where the open joint stock company is the founder of the legal entity — the client; or when there is a multi-level system of ownership of companies located outside the Republic of Belarus;
- in the case where the agreement is signed by an attorney-in-fact or a hired manager who does not have full information regarding a legal entity registered on the territory of the Republic of Belarus and a non-resident legal entity;

- when certifying contracts on the alienation of immovable property, the owner of which is one legal entity, and the founders of this legal entity are also legal entities (identification of the beneficial owner is difficult, since, as a rule, the owner of the property (legal entity) does not possess the incorporation documents of the founder — legal entity, and their provision to a notary for further notarial actions is not required).

Nonetheless, a notary identifies the beneficial owners of clients and verifies the information as follows.

In accordance with the second part of paragraph 5 of the Recommendations for Notaries on Risk Management Associated with the Legalization of Proceeds from Crime, the Financing of Terrorist Activities and the Financing of the Proliferation of Weapons of Mass Destruction, approved by the Resolution of the Ministry of Justice of the Republic of Belarus of 04.10.2016 No. 186, a notary has the right to verify the information provided by the client in case of doubts on its reliability and also to obtain additional information in ways that do not contradict the law. For example, when identifying organizations — to contact the officials of the organization by phone, in writing, including by e-mail; to check information about the head of the organization, another person authorized to act in accordance with the incorporation documents, the person in charge of accounting, other officials who are granted the right to act on behalf of the organization, the founders (members) of the organization, its beneficial owners, and beneficiaries from available databases and data banks, including those in the global computer network Internet.

Thus, a notary can use:

- the information available to them, including publicly available information (Internet resources, mass media);
- the Unified State Register of Legal Entities and Individual Entrepreneurs (hereinafter - the USR), which notaries have access to (they receive information related to organizations registered in the Republic of Belarus from the USR), as well as profiles personal data of the members (founders) of the organization;
- if the organization is not registered in the Republic of Belarus, the notary uses other sources of information to identify the beneficial owners, for example, publicly available mass media, the Internet (in particular, in search engines, they request information about possible access to the register of beneficiaries of the country concerned, information about state registration and the current status of the organization of the country concerned, and information about legal entities and individual entrepreneurs for which documents for state registration have been submitted).

It is also possible to obtain information posted on the websites of authorized bodies of foreign countries. Such websites can contain information regarding taxpayers and tax evaders; open access can be also provided to information about legal entities and individual entrepreneurs, to the registers of beneficial owners which help to identify the ultimate owners of companies, and to other information using which a notary can identify beneficial owners.

However, it must be kept in mind that the information posted on the websites can be uploaded directly by the companies.

The recognition of an individual as a beneficial owner is the result of an analysis of all the documents and (or) information about the client and about such individual, both directly submitted by the client and obtained by the notaries themselves.

The identification of the beneficial owner allows the notary to carry out further internal control measures aimed at:

- determining whether such a person belongs to foreign public officials, officials of public
- international organizations, persons holding positions included in the list of state positions of the Republic of Belarus determined by the President of the Republic of Belarus or their family members and affiliated persons;
- checking whether a person or organization with an individual as the beneficial owner is included in the List of Organizations and Individuals involved in Terrorist Activities, or an organization whose beneficial owner is an individual included in this list.

The List of Organizations and Individuals Involved in Terrorist Activities is available on the website of the State Security Committee of the Republic of Belarus (http://www.kgb.by). In addition, organizations and individuals included in the list are entered in the Unified Electronic System of Notarial Actions and Inheritance Matters Accounting. When the notary enters information about persons participating in notarial actions in the Unified Electronic System of Notarial Actions and Inheritance Matters Accounting, information about whether a person is included in the List of Organizations and Individuals Involved in Terrorist Activities is displayed.

Due to the fact that increasing the transparency of beneficial ownership is a global trend evolving in order to combat illegal financial flows, training events for notaries with the participation of regulatory authorities are conducted systematically. During such events, cases that are non-standard or require multistep actions to determine beneficial owners are studied; notaries learn about new information resources and ways to find the necessary information.

Legal acts regulating notarial activity in the field of AML/CFT are drafted and adopted by the Ministry of Justice of the Republic of Belarus, which is the supervisory authority, taking into account the specifics of notarial activity based on proposals, including those made by notaries.

Activities that cover the maximum available resources allow notaries to most effectively implement in their practice measures aimed at preventing the legalization of proceeds from crime, financing of terrorist activities and financing of the proliferation of weapons of mass destruction.

AML/CFT TRAINING PROGRAMS AND ELECTRONIC SERVICES TO INCREASE THE LEVEL OF INTERACTION BETWEEN THE PRIVATE SECTOR AND THE STATE

Interaction between primary financial monitoring subjects and the state in countering laundering (legalization) of criminal proceeds and terrorist financing is an important aspect of functioning of AML/CFT system

Alexandra Malyarova,
Leading Specialist of the International Training and Methodology Centre for Financial Monitoring

Alexandra Malyarova

To improve the quality of this interaction, the International Training and Methodology Centre for Financial Monitoring develops training manuals on how to use Personal Account of an Entity and educational programs for representatives of the private sector, as well as provides ongoing advisory support for AML/CFT personnel training.

AML/CFT TRAINING PROGRAMS FOR EXPERTS OF ORGANIZATIONS AND INDIVIDUAL ENTREPRENEURS

In accordance with the legal requirements of the Russian Federation, employees of organizations involved in transactions with monetary funds or other assets, as well as individual entrepreneurs specified in Article 5 of Federal Law No. 115-FZ dated August 7, 2001 "On Combating Legalization (Laundering) of Proceeds of Crime and Financing of Terrorism" should receive appropriate AML/CFT training and education.

For more than 10 years, the system of the ITMCFM partner organizations has provided AML/CFT training for experts of organizations and individual entrepreneurs. Such events for the private sector experts contributes to effective mitigation of money laundering risks, including proceeds from corruption and those originating in real estate transactions.

Comprehensive AML/CFT/CPF training includes in-depth study of the basics and principles of operation of the global anti-money laundering system, study of the mandatory AML/CFT requirements stipulated by the national legislation, obtaining information on relevant risks, typologies and schemes of money laundering or terrorist financing.

Last year more than 26 thousand experts were trained on the basis of the ITMCFM partner organizations and more than two thousand events were held, including 9 practice-oriented workshops "Relevant Issues of Compliance with Legal Requirements on Combating Money Laundering and Terrorist Financing by Real Estate Market Intermediaries" conducted in all regions of Russia.

Representatives of the private sector, law enforcement agencies and Rosfinmonitoring took part in the FATF webinar on the results of "Trade-Based Money Laundering" typological research conducted jointly with the Egmont Group.

The ITMCFM and the supervisory unit of the Federal Financial Monitoring Service have arranged a constant exchange of information on individuals who have received AML/CFT training.

Rosfinmonitoring's continuous cooperation with the ITMCFM in the area of training through the ITMCFM partner training centers allows prompt communication of the best AML/CFT practices to the anti-money laundering system stakeholders, focusing attention of the internal control staff on up-to-date ML/TF typologies.

EDUCATIONAL AND METHODOLOGICAL MATERIALS FOR REPRESENTATIVES OF THE PRIVATE SECTOR

The ITMCFM develops AML/CFT educational and methodological materials on the topics of training sessions. They are intended for use in arranging and conducting training activities aimed at training AML/CFT specialists of the Russian Federation and Russia's partner countries. The materials are focused on the need of stakeholders of the national AML/CFT systems for methodological support on the relevant issues related to the main problems of the anti-money laundering sphere.

As part of improving the effectiveness of applying preventive measures and supervisory activities to clarify law enforcement issues to the private sector, the following educational and methodological materials were developed in 2021:

- Identification of politically exposed persons and effective risk management in servicing this category of customers;
- Taking measures to block and freeze funds and other assets without delay.

The ITMCFM website has an updated Media Library section, which contains materials on various topics. The Media Library also contains materials on the organization of interaction between supervisory authorities and the private sector on AML/CFT compliance of reporting entities.

ELECTRONIC SERVICES TO ENSURE OPERATIONAL INTERACTION BETWEEN THE ANTI-MONEY LAUNDERING SYSTEM STAKEHOLDERS

The attention of the ITMCFM has always been focused on the anti-money laundering system, which is being developed in accordance with the international standards defined by the FATF. This system can be presented as a process of combating money laundering and terrorist financing, which consists of several stages.

The initial stage involves the private sector institutions and they are the first to provide a barrier against the penetration of dirty money into the financial system, trying to thoroughly examine the financial integrity of customers and potential partners. In case of suspicion, the financial intelligence unit is informed. The supervisory authorities monitor the compliance of these institutions with their obligations under the AML/CFT law and provisions set forth in other acts. The FIU, in its turn, analyzes the received reports

at the macro level, identifying trends and carrying out ML/TF risk assessment, and conducts financial investigations, disseminating materials to law enforcement agencies when necessary. This is done for the purpose of seizing and confiscating illegally obtained property and income. Each stage has its own mechanism aimed at ensuring the effectiveness of the entire process.

According to the FATF assessment, the mechanisms of the anti-money laundering system, as well as the entire AML/CFT system of the Russian Federation, were recognized as one of the most effective in the world. In this regard, it was decided to implement the study of these mechanisms in the educational process of the INI's member universities and familiarize FIUs of foreign countries with their functional capacity for the purpose of adaptation and integration of similar software products into the national anti-money laundering systems.

In the summer of 2021, the ITMCFM established a digital platform on cloud infrastructure with access via the web interface, where six basic electronic services were launched: National Risk Assessment Center, Personal Account of an Entity, Personal Account of a Supervisory Authority, Personal Account of a Law Enforcement Agency, Transparent Blockchain and "Graphus".

Test boards with electronic services allow FIUs of foreign countries to:

- Identify areas of information and technological development in which the application of the proposed solutions will be most effective for the anti-money laundering system of each country;
- Select from the available options the functionality that will be of most use at the implementation stage;
- Identify the resources required for launching and operating the selected electronic service;
- Arrange the prompt and correct configuration of work processes aimed at implementing the electronic service in daily activities;
- Formulate proposals for the further development of electronic services.

The system of Personal Accounts is a toolkit for operational interaction between all the anti-money laundering system stakeholders:

- Personal Account of an Entity on the FIU website.

The main features of this service allow institutions involved in transactions with monetary funds or other assets to send suspicious transaction reports to the FIU via encrypted communication channels and have online access to up-to-date lists of TF and PF-related persons, and the FIU – to inform entities about the current compliance risks and take preventive measures.

- Personal Account of a Supervisory Authority on the FIU website.

The Personal Account of a Supervisory Authority provides operational information about the risks in the supervised sectors and in the activities of specific organizations.

- Personal Account of a Law Enforcement Agency on the FIU website.

The Personal Account of a Law Enforcement Agency was developed to arrange information sharing with law enforcement agencies in electronic form, which allows quick electronic information sharing, including mutual reviewing of materials and exchange of statistics and analytics when assessing the situation in the AML/CFT sphere.

In 2022, in accordance with the decision of the 35th EAG Plenary meeting (November 2021), the ITMCFM will provide registration of personal accounts, as well as access to the Media Library materials to interested FIUs and will continue uploading relevant materials on interaction between the private and public sectors to the Media Library.

EXPERIENCE OF "ORIENBANK" OJSC (TAJIKISTAN) IN THE AML/CFT/CPF FIELD[1]

Khurshed Salomov,
Head of Compliance Division at "Orienbank" OJSC (Tajikistan)

Khurshed Salomov

Each credit institution in the normal course of daily business encounters ML/TF/PF risks and each financial institution must take reasonable and justified risk mitigation measures if it intends to retain client credibility in the future, to expand its business by means of increasing the number of branch offices and service points, to avoid image risks (i.e. avoid having business with dubious clients, operations or transactions that may impact bank's reputation), retain the credibility of foreign correspondent and partner banks and avoid getting heavy fines from the regulator (in case of serious breaches the regulator may revoke the license of a credit institution to carry out banking activities). Orienbank is not an exception.

Orienbank collects client data as part of internal control activities by carrying out surveys, conducts client identification and verification, checks clients against available lists of terrorists and extremists and against sanctions lists, determines the purpose and nature of business relations of the client with the bank, makes an analysis and assessment of risks inherent to this client and takes reasonable and justified risk mitigation measures. In the bank a risk-based approach is applied (most of AML/CFT/CPF resources are channeled to high risk clients and therefore such clients get subjected to more thorough monitoring, while low-risk clients require smaller amount of resources).

In order to minimize the ML/TF/PF risks the bank takes the following action:

1) apart from mandatory client identification, client verification is also carried out; client screening is conducted in international fee-paying search information databases for any illegal action committed by such client, and prior to deciding whether an account could be opened for the client a search is conducted for possible negative information on the client based on public sources of information (the Web, mass media publications, etc.).

[1] Prevention of Legalization (Money Laundering) of Criminal Proceeds, Terrorist Financing and Proliferation Financing.

2) respective modules for the ultimate client risk (high/low) assessment are integrated as part of a mandatory KYC (Know Your Customer) procedure based on earlier uploaded information on the nature of the client's activities, the client's sources of funds, anticipated turnovers on the client's accounts, etc. according to Appendix No. 1 to Instructions 171 of Tajikistan's National Bank 'Procedure for Opening, Renewal and Closing Banking Accounts at Credit and Financial Institutions in the Republic of Tajikistan'.

Based on the assessment, a decision is taken for the frequency and the depth of client transaction monitoring and the required frequency of updating information obtained in the course of the client and beneficial owner identification (in case the client is classified as high risk, the client is more frequently subjected to enhanced monitoring and client information is updated at least once a year; in case the client is classified as low risk, the bank conducts less thorough monitoring of such client, and client information is updated at least once every three years) as required by Instruction 200 of Tajikistan's National Bank 'On the Identification and Verification of the Client and Beneficial Owner'.

Client risk levels are not permanent and invariable values and can be revised as client identification data changes or as respective conclusions are drawn on the outcome of monitoring and analysis of transactions completed by the client.

3) respective modules for screening against terrorists and extremists lists and sanctions lists are introduced for spotting the client in such lists and alerting competent authorities if any match is found (if a full match is established, the system blocks the transaction and freezes the client's funds) prior to execution of any transaction, including opening a bank account for the client (money transfers of physical persons without opening a bank account, incoming transfers to the client's cards, sale and purchase of foreign currencies, payments made by the SWIFT receipt and execution system, etc.), and also modules are provided to stop transactions, in case when payment details contain unacceptable words (drugs, weapons, etc.).

4) the bank always informs the regulator of suspicious transactions where this or that transaction gives rise to suspicion. The Bank on a daily basis submits to the regulator information on transactions subject to mandatory control (transfers by individuals without opening bank accounts, crediting/debiting of/from client account (accounts), payments via SWIFT, purchase/sale of foreign currencies).

5) if following in-depth monitoring the bank will have some doubts as to the legitimacy of transactions performed by the client, the bank will be bound to send suspicious transactions reports, conduct a full inquiry requesting customs cargo declarations (CCD) for payments and upon completion of the inquiry, a decision is taken whether to continue relationship with the client or fully close accounts of the client.

6) the bank focuses its attention on transactions performed by clients who are classified as politically exposed persons (PEPs) or public service officials (PSOs). PEPs (PSOs) clients are not taken on board unless a written authorization to that effect is issued by bank's (deputy) manager. Subsequently their transactions undergo thorough monitoring and the bank takes reasonable and justified measures for identifying sources of funds and property owned by such clients.

7) the bank has set up the formation of automatic reports to provide necessary monitoring of transactions, as well as to provide timely response to inquiries from the financial intelligence unit (FIU).

8) the bank has developed required rules and policies: the Internal Control Rules for Preventing Legalization of Criminal Proceeds (Money Laundering), Terrorist Financing and Proliferation Financing (AML/CFT/CPF); the Policy for Preventing Corruption, Corporate Fraud and Concealing Information on the Conflict of Interests; the Policy for Preventing Legalization of Criminal Proceeds (Money Laundering), Terrorist Financing, Proliferation Financing and Extremist Financing and the Compliance Risk Management Policy.

9) the bank's employees provide regular training in the AML/CFT/CPF area to front office personnel comprising first 'defence' line, and when changes to the legislation are made, necessary information is promptly disseminated to respective bank employees.

The existing arrangements and controls at Orienbank allow minimizing the ML/TF/PF risks. What is the reason for using the term 'minimizing'? The reason is that the ML/TF/PF risks cannot be fully excluded.

AML/CFT/CPF POLICY AT "ALIF BANK" OJSC

Umed Pochoev,
Head of Compliance Division of "Alif Bank" OJSC (Tajikistan)

Umed Pochoev

In its operations, Alif Bank abides by the principle of avoiding the use of the Bank's products and services for money-laundering, terrorist financing and proliferation financing. The Bank condemns terrorism in all its forms and manifestations and strongly opposes any transactions that lead to money laundering, terrorist financing and proliferation financing.

The Bank takes necessary CDD measures in relation to its clients (their representatives) and beneficial owners; carries out financial monitoring procedures of its clients' transactions; does not establish or maintain correspondent relationship with shell banks and banks that completely or partially do not apply AML/CFT/CPF measures.

Pursuant to 'Know Your Client' procedures, prior to establishing business relations, the Bank requests from the client all necessary documents and personal data on individuals and information on legal entities as required by regulations and statutes of Tajikistan's National Bank. All received information is contained in the 'Client Questionnaire' that is to be kept in the client file. This information is used for client classification according to the risk level. Client information is to be updated from time to time depending on the risk level. The Bank on an ongoing basis monitors business relationships and thoroughly reviews client operations and transactions.

Also, acting under the aforementioned procedure and with the objective of minimizing risks of using products and services, the Bank performs client classification according to the risk level. The client assessment is made based on such criteria as geography(country), type of activity, residence, client's belonging to PEPs (politically exposed persons) and presence of the client (or his/her relatives) in the list of persons linked to terrorism and EC, UN, and OFAC sanctions lists. The client transactions monitoring findings also affect the overall client risk assessment.

If there is a suspicion that a transaction may be performed with the aim of money laundering, terrorist financing and proliferation financing the Bank's employee presents all transaction details to an authorized officer. Upon analysis of information received and when deciding to block a transaction, the authorized officer gets in touch with an employee of the Financial Monitoring Department at the Tajikistan's National Bank (FMD at TNB), submits to him or her all information and awaits further instructions. Subsequent steps are taken in coordination with the employee of FMD at TNB. If the Bank's client is included in the list of entities and persons connected with terrorist and extremist financing or the Sanctions Lists after business relations are established, such clients will be subject to procedures provided for in the laws of the Republic of Tajikistan and the Bank's internal regulations.

In order to avoid its personnel's involvement, the Bank provides AML/CFT/CPF training and education and all information on the AML/CFT/CPF legal requirements in the Republic of Tajikistan, normative legal acts of Tajikistan's National Bank and also of international organizations. The personnel training procedure consists of two courses. The introduction course includes training in basic knowledge of the AML/CFT/CPF legislation of the Republic of Tajikistan and the Bank's internal regulations; the main course – training of the Bank's personnel, introduction to normative legal acts of Tajikistan's National Bank, international and domestic requirements.

Implementing relevant legislation requirements the Bank submits information on transactions subject to mandatory control and on suspicious transactions within a timeframe established by the competent authority. The list of indicators of suspicious operations and transactions is presented in the 'Register of Suspicious Operations and Transactions' approved by the competent authority.

Other important goals of the Bank are aligning the activities of the Bank and employees with the laws of the Republic of Tajikistan and the normative legal acts of Tajikistan's National Bank in the field of AML/CFT/CPF and setting up and operating the internal control system and the money laundering, terrorist financing and proliferation financing risk management system.

To achieve the targets, the Bank develops and implements internal regulations, updates them when necessary and assures the involvement of the Bank's employees in internal controls for the purpose of AML/CFT/CPF with a clear division of functions between employees in the internal control system. The Bank's personnel provides assistance to authorized officers in exercising their functions and on operational issues related to client transactions posing to the Bank high risks of money laundering, terrorist financing and proliferation financing.

ROLE OF NON-CREDIT FINANCIAL INSTITUTIONS IN AML/CFT

Svetlana Lysenok,
Deputy Head of Financial Monitoring Methodology Division of the Banking Supervision Chief Department of the National Bank of the Republic of Belarus

Svetlana Lysenok

The current stage of development of the system for preventing money laundering, financing of terrorism and financing of proliferation of weapons of mass destruction (hereinafter AML/CFT) is marked by its gradual and steady integration into the financial sector of the Republic of Belarus, which results in rapid expansion of the control area of the public authorities.

At the moment, the National Bank is regulating the AML/CFT activities of the following non-credit financial institutions:

- Leasing institutions;
- Microfinance organizations, other legal entities having legal right to perform microfinance activities, including buy-up points (relates to their microfinance activities);
- Forex companies, the National forex center, banks and non-bank credit and financial institutions (relates to their activities of conducting transactions in non-deliverable off-exchange traded financial instruments initiated by individuals and legal entities - Forex market activities);
- Operators of online borrowing services.

According to the Law of the Republic of Belarus «*On Measures for Preventing Money Laundering, Financing of Terrorism and Financing of Proliferation of Weapons of Mass Destruction*», which is the key normative legal act in the area of AML/CFT, the above mentioned entities are the parties carrying out financial transactions.

Thanks to the activities of the National Bank and concerned associations, non-credit financial institutions have developed understanding of the importance and need of compliance with AML/CFT laws: there have been fewer violations of AML/CFT rules, sectoral normative acts of organizations are being actively improved.

Participation of representatives of non-credit financial institutions in the mutual evaluation of the AML/CFT system established in the Republic of Belarus for compliance with the FATF international standards has become a major event for non-credit financial institutions.

Assessment was performed from September 2018 till November 2019 by the Eurasian Group on Combating Money Laundering and Financing of Terrorism (EAG). Results of this assessment have produced a significant effect on the process of further operation of the financial system of the Republic of Belarus.

The assessment also involved representatives of the private sector. Conclusions of international experts reflected in the Report on Mutual Evaluation were based, among other things, on the opinion of representatives of non-credit financial institutions reflecting their understanding of AML/CFT legal requirements and efficiency of compliance with them.

The country obtained high ratings thanks to the concerted efforts of public authorities (law enforcement and supervisory authorities) under the general guidance of the Public Control Committee of the Republic of Belarus, as well as banks, non-credit financial institutions, and other financial institutions.

ARRANGEMENT OF REMOTE CONTROL OVER NON-CREDIT FINANCIAL INSTITUTIONS

Considering the scope of the non-credit financial transactions sector, the results of the national assessment of money laundering and terrorist financing risks, as well as the mutual evaluation of the Republic of Belarus, the National Bank has faced the need to use the right granted by Article 16 of Law No. 165-Z to establish for non-credit financial institutions forms of reporting financial transactions and/or clients subject to identification and information on AML/CFT activities of such entities.

We believe that understanding the risks and weaknesses inherent in AML/CFT control at the sector level is the starting point for understanding the risks at a more detailed level, i. e. at the level of individual parties. To identify the risk in every sector as a whole, it is necessary to take into account the nature of business models used in the sector, as well as activities and risk profiles (e. g., scopes of activity, specifics of the client base) of the sector parties.

Transition from the rules-based supervision to the risk-based supervision takes time and can be challenging. This requires changes in the culture of supervision. The National Bank closely cooperates with the private sector to get a deeper insight into the risks faced by the regulated entities. This is important since every business operates differently and faces different risks.

The practical communication by the regulatory authorities to the business community of clarifications concerning the framework of exercising by financial institutions of the right to refuse conducting financial transactions that have signs of money laundering and financing of terrorism, with provision of specific examples (cases), appears interesting. Raising awareness among representatives of this sector of the AML/CFT legal requirements allows them to address more efficiently the situations where non-credit financial institutions apply enhanced due diligence measures, or to justify that there is no increased risk in conducting any given transaction. On the other hand, this allows to lower the number of derisking cases where financial institutions formally or unreasonably stop or restrict business relations with certain clients or categories of consumers in order to avoid the risks of being involved in dubious schemes.

ARRANGEMENT OF REMOTE TRAINING

Heads of entities must have the relevant powers, skills and resources, as well as political and administrative support. They need to constantly update their understanding of risks and to adjust and improve their approach to the supervision[1].

[1] https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-supervision.html.

In order to accomplish these tasks, in December 2020, the National Bank established a remote training portal for non-credit financial institutions at the official website of the National Bank Training Center for uploading AML/CFT training materials and presentations.

A Personal account has been created for every entity carrying out financial activities in the name of its director. The portal is designed for training an unlimited number of the entity employees according to the procedure established by the local normative act of the relevant entity.

The obligation of executive officers of the entity carrying out financial activities to take annual training in AML/CFT is set forth in the regulation of the National Bank. The National Bank controls compliance with this requirement remotely, as well as at the time of on-site inspections.

CONCLUSION

The contemporary risk-based approach to control over AML/CFT activities of non-credit financial institutions will enhance the efficiency of the efforts of supervisory authorities to identify and disrupt financial flows feeding crime and terrorism. It is very important since identifying and preventing money laundering and terrorist financing is more preferable than conducting prosecution after commission of a crime.

PROMPTLY RESPONDING TO THE EMERGENCE OF NEW CHALLENGES AND THREATS

The Compliance Council platform in the Southern Federal District provided an opportunity for close interaction between financial institutions and Rosfinmonitoring Interregional Department for the Southern Federal District (hereinafter the IRD), which allows to ensure that there is sufficient understanding of the goals of the anti-money laundering system, as well as of the risks of their involvement in illegal schemes and the importance of reducing vulnerability to them

German Shatsky,
Head of Rosfinmonitoring Interregional Department for the Southern Federal District

German Shatsky

The systematic monitoring of the events being implemented under the auspices of the Council allows the IRD to respond to deficiencies identified in the work of financial institutions by taking timely mitigating measures.

Among the significant tasks implemented by the Council, the IRD highlights the mechanism for risk orientation of control, supervisory and law enforcement authorities. Thus, information exchange with regional members of the Compliance Council allows timely monitoring of social tensions in the context of current realities, as well as promptly responding to the emergence of new risks and threats.

Apart from the Compliance Council, the IRD is involved in arranging and conducting individual events for representatives of the private sector, using all available formats: workshops, webinars, consultations, scientific and practical conferences, etc. In 2021, for the purpose of increasing the level of participation among the organizations (individual entrepreneurs) providing intermediary services in

real estate sale and purchase transactions, events in the format of webinars for representatives of the real estate sector were held in the AML/CFT system on a quarterly basis. Consultations on sectoral risk assessment were also provided for representatives of each sector. The mentioned events allowed reaching a qualitatively new level of interaction with the sector.

In the first quarter of 2022, events in the format of webinars for representatives of payment acceptance operators and leasing companies were held, as well as individual consultations with each representative of the specified sectors. The application of such formats had a positive effect on the law-abidance of supervised entities. The level of law-abidance of the leasing sector increased by 0.3%, the share of payment acceptance operators who use their Personal account to view/download the List – by 9.2% and the share of payment acceptance operators who submit customer verification reports (3FM Form Report) – by 4.6%.

Moreover, using the aforementioned formats of interaction, it was possible to update the subjectivity of organizations registered with Rosfinmonitoring (those not involved in supervised activities received recommendations to deregister).

THE RANGE OF PARTICIPANTS OF OUR DISCUSSION PLATFORM HAS EXPANDED BOTH QUANTITATIVELY AND GEOGRAPHICALLY

The Compliance Council in the Siberian Federal District operates pursuant to and in accordance with the Regulations of the Compliance Council, approved by the Director of the Service on 6 July 2016

Nikolay Buymov,
Head of the Interregional Department of the Federal Financial Monitoring Service for the Siberian Federal District

Nikolay Buymov

When exercising its powers to organize and conduct meetings of the District Compliance Council, the Department is guided by the recommendations of the Directorate for the Organization of Supervisory Activities and focuses the activities of the Regional Compliance Council (hereinafter - the "RCC") on issues related to identification of new ML/TF risks (schemes), improvement of the quality of STRs and sharing best practices on challenging issues of AML/CFT law enforcement.

The forced measures related to conducting events via videoconferencing in 2020 due to the epidemiological situation have subsequently opened up opportunities to arrange RCC meetings promptly, and most importantly to expand the range of participants of the discussion platform not only in quantitative terms, but also in terms of geography.

Thus, meetings of the banking group are held involving all regional banks, as well as representatives of branches of the major credit institutions at the federal level.

The notary sector in the RCC is represented by the presidents and staff of the territorial notary chambers, the most active notaries of all regions of the area, and moreover, if necessary, employees of the departments of the Ministry of Justice of Russia are also invited.

The leaders of the professional associations of real estate agents participate in the meetings of the thematic group of real estate intermediaries. The Department has entered into cooperation agreements with nine associations of real estate agents in Siberia, within the framework of which training events and workshops are held and the associations' websites provide up-to-date information on AML/CFT issues. Last year 2021, in order to mitigate the risks of involving real estate agents in unlawful activities, being among the representatives of the Novosibirsk real estate agency market, N. Morozova, Director of the Novosibirsk branch of the Federal State Budgetary Institution of Higher Education "Moscow Academy of the Investigation Committee of the Russian Federation" made a report on "Criminal law risks when carrying out real estate agency activities" at the meeting of the RCC.

Intelligence emerging in the district is exchanged with the participants of the RCC on a routine basis. Discussions at the RCC meetings of various internal control practices provide an insight into and assessment of both potential risks and vulnerabilities observed by Council members. Thus, the issues raised at the meeting on cashing-out of funds through the sale of trade revenues took the form of a typology, which became available to all participants of the counteraction system by posting it in Personal accounts on Rosfinmonitoring's website.

TYPOLOGIES, METHODS AND TOOLS FOR IDENTIFYING ILLEGAL ACTIVITIES IN THE FINANCIAL MARKET

Dmitry Gronin,
Head of the Internal Control Service, NPO "UMoney" LTD

Elizaveta Demidova,
Head of the Financial Monitoring Department, NPO "UMoney" LTD

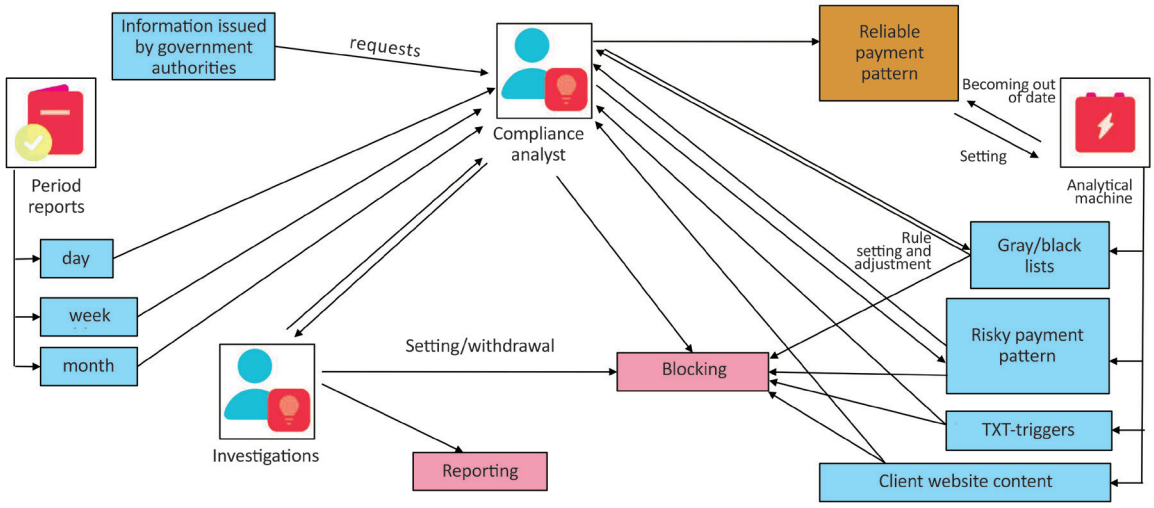
Dmitry Gronin

Elizaveta Demidova

In the digital economy era, advanced banking payment services both for personal transactions of individuals and business entities receive a lot of development. Easy connectivity and use, prompt online calculations, and available support not only to money flows, but also to complex information exchange place high requirements on regular monitoring, timely assessment of clients and their activities by a credit institution, as well as on prevention of illegal financial transactions with a view to both protecting the reputation of the service itself and reducing client risks when establishing relationship with unscrupulous counterparties. To that end, there is a need to apply organizational methods and automated means, including analytical machine algorithms embedded with artificial intelligence and machine learning elements.

The tool, which is at disposal of a credit institution's financial monitoring unit, comprises reports and samples on the most risk exposed criteria (cashing-out, transit and transfer abroad) regularly uploaded by staff, as well as constantly running analytic algorithms responding online without employee involvement (Fig. 1). Specifically, the analytical machine operates an extensive range of regularly

Fig. 1: Tool analysis of client behavior and profile



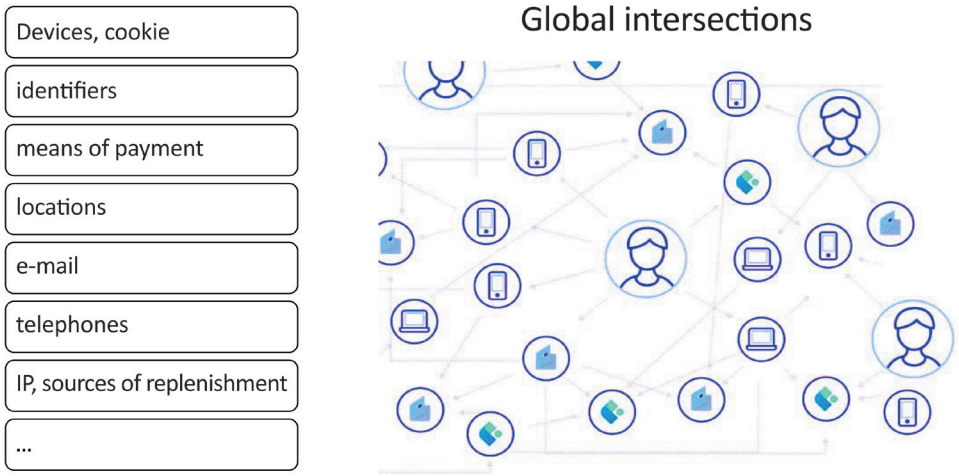
updated gray/black lists, complex rules of describing a reliable and risky pattern of payment behavior and rules of responding to various text triggers as part of an information flow accompanying a payment, as well as client website content analysis algorithms and related forms.

We believe that the starting point of analysis and application of some special algorithms is a clear segregation of banking products and services into personal and business ones. It allows not only approaching correctly to selection of the analysis method, but also to avoiding the risk of disrupting the operation of bank accounts held by individuals, as well as of electronic payment means (EPM) that are not classified as corporate ones. So, for example, the UMoney-wallet service of the NPO "UMoney" LTD is officially positioned as a means of exclusively personal non-business transactions made by individuals, while the client offer contains a direct ban on business payments. Therefore a substantial focus when assessing clients and their payment behavior in monitoring of personal products is given to identification of covert penetration facts serving the needs of illegal business entities. In fact, such developments account for the main volume of prevented illegal activities in equal measure related both to the illegal nature of products and services, as well as to trade in legitimate products by entrepreneurs trying to evade government registration and taxation. The business activity identification tool set operates selected data regularly uploaded by personnel and machine algorithms in a prompt response unit, most of which are primarily correlated with the rules of the Methodological recommendations of the Bank of Russia No. 16-MR dated September 06, 2021 (a substantial number of operations and counterparties, regularity, repeatability, a high frequency of operations, a short time period of account inactivity, a small balance amount, etc.). In addition, constantly running algorithms are applied to identify interrelated sets of clients and accounts that have no formal connections but are integrated into unified group by indirect indicators some of which are shown in fig. 2.

Regarding banking products initially designed for business transactions (cash and settlement services, acquiring, etc.), legitimacy of ongoing activities of a client is reviewed both in the course of customer onboarding and regularly during the provision of such services, including examining client changes (with regards to the profile, activity, website and other parameters requiring attention). Applied on a daily and per transaction basis, automated algorithms allow identifying and controlling:

- any appeals or feedback at online independent customer review websites reaching a credit institution indicating the illegitimate nature of client activities/website or the need for special regulation;

Fig. 2: Identification factors of global intersections



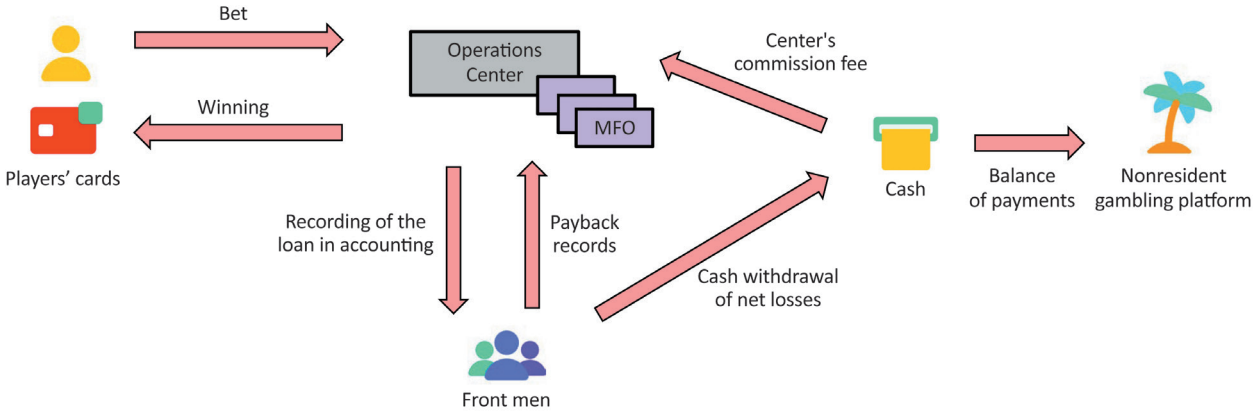
- interrelations with a database of previously identified customers engaged in illegal activities in reference to managers, representatives, and owners; digital footprints of applied devices and IP-addresses of primary network access; recorded cookies, phone numbers, e-mail addresses, patterns of created logins, and locations of ATM and terminals, etc.;
- substantial interrelations of payers between various stores formally owned by independent persons having no signs of any relationship;
- substantial changes in the content of a website hosting payment forms, including emerging words and word combinations indicating illegitimate or licensed or specially regulated products and services;
- the turnover and average purchase amount exceeding the limits typical of the stated activity or failing to match the range of products and services listed on the client's website;
- other trends in payment behavior on patterns typical of previously identified clients engaging in illegal activities, other payment anomalies based on payment amounts, frequency, locations and other factors.

Attempts of carrying out illegal activities in the financial market account for a significant portion of a total of actually identified illegitimate business schemes: on-line casinos, cryptocurrency exchange, pyramid schemes, pseudo-educational Internet-projects, illegal lending, etc.

One should note essential efforts regularly made by the Russian legislator to progressively oust out of the national financial system certain payments for products failing to meet the national regulatory requirements that are frequently sold by foreign business agents posing threat to the financial security of consumers of such services, primarily Russian nationals. The Federal Law No. 355-FZ dated July 02, 2021 established as AML/CFT requirement earlier actually existing practice of verification of customer activities which fall under Russian licensing requirements. The legislation on regulating gambling and lotteries management activities was made more and more stringent. Thus, the Federal Law No. 358-FZ dated November 27, 2017 introduced the black lists of violators of regulatory requirements drawn up by Russia's FTS (Federal Tax Service). The Federal Law No. 355-FZ dated July 02, 2021 clarifies that Russian regulations should also be applied based on whether the users of gambling platforms have any links with the Russian jurisdiction, specifically, that concerns the domicile, bank location, IP-address and telephone number, which actually prevents Russian users from receiving gambling services from foreign organizers bypassing the system of Interactive Bets Accounting Center (IBAC).

With regard to the practice of suppressing certain widespread typologies of illegal activities in the financial market, it is necessary to highlight a number of features.

Fig. 3: A casino's shadow processing center operations



1. Online Casino

In the context of the latest changes in regulatory control of gambling and lottery management that have established the need for executing control over the signs of links with Russia, including foreign gambling platforms outside Russia, the role of the FTS black lists becomes less critical since such links related to their clients are detected by credit institutions much faster than in the listing process. Covert penetration of illegal platforms for banking servicing is countered by the simplicity and speed of their identification using such criteria as the volume, frequency and high number of transactions with a wide set of payment instruments available to individuals. A new stage of such penetration was characterized by attempts of disguising gambling traffic as functioning of industries with similar payment patterns, choosing microfinance activity as the most suitable one. Such microfinance organizations apply for onboarding under the pretext of proceeding with their existing operations, having concealed software program integration with gambling organizers' websites and accepting online bets under the guise of micro-loan repayments and paying out winnings in the form of lending. Net losses of players in the form of such loans are channeled to a limited list of cards held by front men (drops) to withdraw cash and transfer it to casino owners with the deduction of a commission fee (Fig. 3). The facts of such cash withdrawals are difficult to detect by monitoring means in the general flow of transactions across the entire client base. Generally, the automated analysis tools of the microfinance organizations payment pattern also prove to be of little use since identical average transaction amounts, high volume and frequency, and a wide range of clients are an integral part of the modern online microfinance industry.

An in-depth inspection of similar microfinance organizations uncovers the following negative criteria:

- limited personal data of borrowers to whom micro-loans are issued on a daily basis or more frequently with the overall amount of debt exceeding the statutory limits;
- the localization of considerable peak amounts in the limited scope of payment details used for cash withdrawals;
- the signs of falsifying applicable reporting

Frequently cross-requests forwarded to individuals, i.e. microfinance organizations counterparties, make it possible to confirm a hypothesis about interrelations with illegal casinos and identify their websites, as well as carry out an on-site inspection and document findings obtained. Also, the identification of such unscrupulous microfinance organizations also allows marking the payment details of players involved for subsequent prompt exposure of any similar schemes.

2. Crypto exchangers

Illegal organizers of cryptocurrency exchange practically don't use bank's business segment services. The key target of penetration is accounts and e-wallets of individuals where an illegal exchanger is identified and closed, primarily based on the criteria of Methodological Recommendations of the Bank of Russia No. 16-MR dated September 06, 2021, in the

overall flow of illegitimate entrepreneurship. In some cases, it becomes possible to qualify them more thoroughly as an exchange service according to the following criteria:

- a relationship along various visible factors with earlier closed clients qualified as exchangers;
- the payment flow is characterized by a high specific weight of counterparties of earlier closed clients qualified as exchangers (a database of earlier identified payment details of private cryptocurrency sellers and buyers is used);
- there are two and more independent complaints of making exchange activities or applications on other subjects, however giving an indication of the true substance of the client's activities.

3. Pseudo-Educational Projects

Such projects are for the most part identified based on the findings of the content analysis of a website offering training courses and classes with certification. The absence of an education license is disguised by a variety of agreements with licensed educational institutions that are intended to provide training to the client itself and its personnel and are not classified as agency one in substance, don't envisage the involvement of university professors in education process. Order of the Ministry of Science and Higher Education of the Russian Federation No. 882 and the Ministry of Education of the Russian Federation No. 391 dated August 05, 2020 sets out the Procedure for Organizing and Conducting Educational Activities as part of the network form of implementation of educational programs which has determined the opportunity to an unlicensed partner (resource) entity to participate in the educational process. A note should be made of more frequent onboarding penetration attempts of unlicensed entrepreneurs and entities under the cover of an agreement for educational activities in the aforementioned network form where a 'resource' entity tries on its own to organize an education process.

Summing up the reviewed schemes, it should be noted that effective identification and prevention of illegal practices is becoming possible not only on the basis of results of inspection of a license regime, but also on the basis of reviewing a number of regulatory control details of a specific type of activities with application of the automated tools. Organizational and program methods of reviewing client payment behavior and external source information enable prompt identification, classification and suppression of the aforementioned illicit schemes along with raising relevant information awareness of competent authorities.

IMPROVING FINANCIAL LITERACY

IMPROVING CUSTOMERS' FINANCIAL LITERACY AS A TOOL TO REDUCE AML RISKS

This article is focused on the issues of mitigating the risks of conducting dubious transactions in a not quite standard way, namely through the understanding by a financial organization of its social responsibility, conducting systematic outreach work with its clients

Aidar Bagaviev,
Compliance Director of "AK BARS" BANK PJSC

Aidar Bagaviev

All existing market stakeholders engaged in dubious activities can be divided into two categories: "rogues" who are well aware of what they are doing, what they are risking and what laws and requirements they are breaking, and "simpletons" who may not realize what they are engaging in and the consequences of such engagement. And the demand for the latter from the former has recently increased manifold.

While it used to be easy enough to distinguish unscrupulous market players from the healthy part of the market - the elementary criteria of shell companies worked out, today more and more often unscrupulous persons try to take advantage of the low literacy of others and involve representatives of real businesses and individuals with spotless reputation in their activities.

Fig.1. Features of the blurring of the lines of shell companies

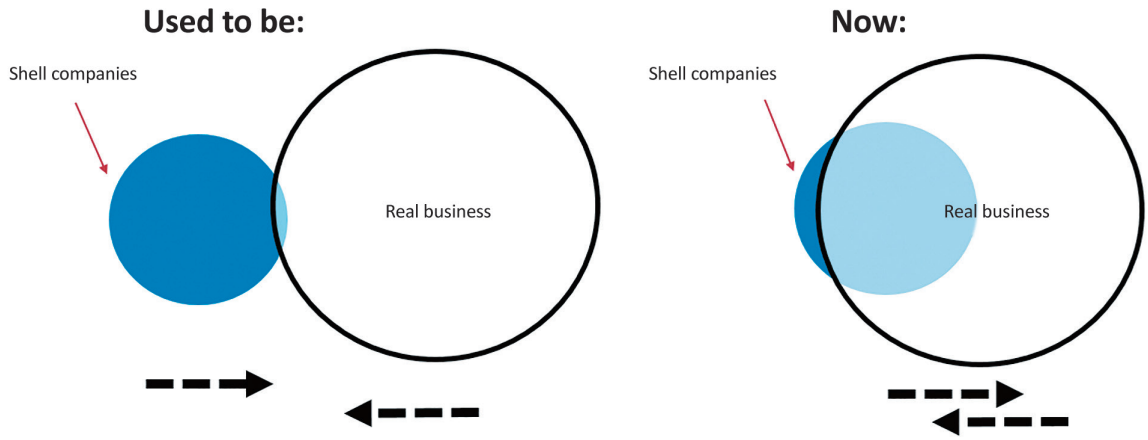
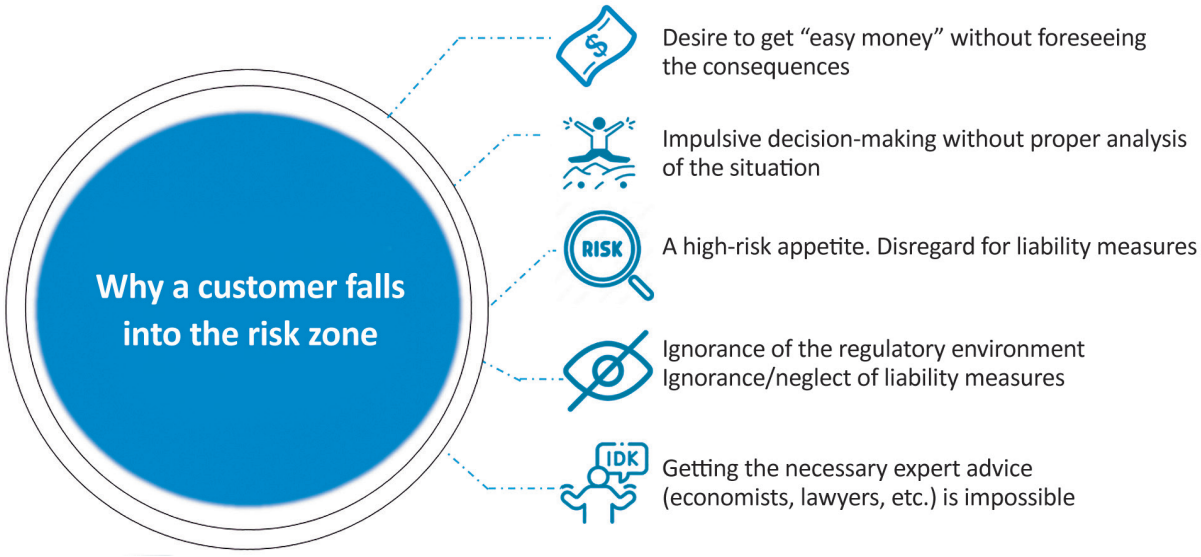


Fig. 2. Prerequisites for the involvement of persons with low financial literacy in money laundering schemes



As shown in the figure 1, the division into black and white used to be quite clear, and the "grey" area was quite insignificant. Today the situation is drastically different, and the major part of suspicious transactions take place right there.

It is notable that, according to official statistics, in the last 3 years the number of registered legal entities with signs of shell companies has dropped from 1.5 million to 0.12 million - that is, by nearly 14 times. Taking into account the developments and the relocation of unscrupulous participants, it can be affirmed that the volume of suspicious transactions has decreased in much smaller proportions over the period.

The reasons why customers may become involved in dubious schemes are varied and obvious to many.

To one degree or another, these qualities are common to all people, but all these prerequisites can be underpinned by the low financial literacy of market stakeholders and this is what the financial monitoring units of credit institutions have to deal with.

There is a number of schemes, in which individuals and legal entities not being aware of the risk of their actions can take part. The most common are rolling cashing-out, sale of cash proceeds, corporate card transactions, VAT scrambling, mass opening of drop cards, etc.[1].

Credit institutions are certainly trying to take into consideration the current realities and are developing new and more effective methods and tools to combat unlawful activity. But it must be admitted that the current tools are not enough. Although the national AML/CFT system has made a great progress in this fight and has reduced the volume of suspicious transactions manifold, a quality leap is required for the next breakthrough in terms of awareness of those AML/CFT functions, the request for which has already been formed by the market, but which have not been given as much attention so far. This is primarily a question of the outreach function of the financial monitoring units of credit institutions.

Banks should act as a guide to their customers and explain which transactions are unacceptable and what risk management measures can be taken. It stands to reason that such work should be done before a person or organization is involved in engaging in illegal activity.

A financial institution can approach the implementation of this function in many ways. The most feasible approach would be for the bank to focus on creating a framework on which the relevant functionalities are based before applying specific measures and tools in its work with customers and other market participants to improve their financial literacy.

They should not start with the customers, but with the processes within the credit institution. In order to give customers a proper explanation of what they can do and what they should guard against, employees dealing with customers need to have a good understanding of the essence of the state of things and be fully aware of the responsibilities of the bank. For this purpose, a program to foster a compliance culture can be created within the bank. It can include a variety of information campaigns (targeted videos, posters should be created, competitions should be held, etc.) Training courses should be conducted on a permanent basis (in all formats - face-to-face, remotely, interactively). It is crucial that communication also comes directly from the bank's CEO. Communication channels with compliance should be developed (employees should have information about where and how they can raise issues). All of this is aimed at strengthening the principles of responsibility in the minds of employees, which would enable them to interact with customers in a more efficient and sustainable way.

> *Improving financial literacy of customers begins with establishing rules, a way of thinking and raising awareness among bank employees.*

Once all staff within the bank have been "energized" with the necessary enthusiasm and knowledge, the awareness-raising dialogue with customers can be initiated.

One of the most effective ways of communicating information to customers is through the development of various information and analytical resources where bank employees act as experts, provide market assessments, and advise both current and potential customers on issues of interest to them. The best way to improve the financial literacy of bank customers is to conduct outreach to target groups of customers interested in gaining financial knowledge, including basic financial market trends and the specifics of banking services. According to NAFI (National Agency for Financial Research) Analytical Center, 83% of financial companies provide training to employees, 43% provide customer training, product descriptions (36%) and contracts (34%) are made easy to understand. In addition, 90% of financial institutions provide customer consultations at branches, 53% post information articles on their website and 36% disseminate printed information materials.

[1] Typologies of dubious money laundering schemes are presented based on the press service data of Rosfinmonitoring (https://www.fedsfm.ru/).

A useful innovation in the work is the introduction by banks of internal services such as the "Compliance Assistant", "Safe Business", and "Auditor", which allow customers to self-assess their level of compliance risk and see which of their actions could lead to negative consequences. It is worth noting that such resources should not become a tool to evade or defraud the credit institution's controls, which could have been exploited by unscrupulous market participants.

In order to build trust relationships with customers, banks should also hold “Open Doors” Days at their offices, publish expert advice, and actively interact via social media.

All these events should contribute to developing motivation of customers in improvement of their financial literacy due to their inability to orientate themselves in the variety of "ways to make money" available in the market and help them make informed decisions when making transactions.

Customers' financial literacy is, without exaggeration, the keystone of sustainable development in our economy. We need to understand this, be aware of it and make the necessary efforts to work with market participants. Issues of improving financial literacy should be implemented in the ESG agenda of each bank.

IMPROVING FINANCIAL LITERACY WHEN INVESTING IN DIGITAL ASSETS

Aidar Beknazarov,
Senior Compliance Manager, "Quantdart Fintech Limited" Private company

Aidar Beknazarov

Since June 2020, a number of amendments have been introduced into Kazakhstan's legislation, recognizing digital assets as a type of property. The legislation distinguished between secured and unsecured digital assets.

No turnover of unsecured assets (which include bitcoin and other crypto assets) is allowed within Kazakhstan, they are only allowed to be bought, sold and held through members of the Astana International Financial Centre (hereinafter - the "AIFC").

New technologies, high volatility, enhanced anonymity, decentralization and remote establishment of business relationships carry high risks of exposure to cryptocurrencies being used for the purposes of money laundering, terrorist financing and proliferation of weapon of mass destruction.

In this regard, clear regulation of activities related to the purchase, sale and holding of digital assets is a reliable mechanism to prevent crime and to avoid escalation of social tensions.

The AIFC Financial Services Regulatory Committee, when licensing digital asset companies, takes a comprehensive set of measures aimed at protecting retail consumers of financial services from loss of investment capital. Limits have been developed on

both the volume of customers and the maximum amount of digital assets that can be held in a wallet for each type of customer. Requirements for conducting financial and information security audits have been established. Separate storage of customer fiat money and digital assets apart from customer monetary funds and digital assets is envisaged.

The Financial Monitoring Agency has developed indicators of suspicious transactions, a mentoring institute has been established and a regular dialogue has been built within the Compliance Council to further develop typologies and requirements for internal control rules for companies and other AML/CFT issues related to the turnover of digital assets in AIFC sphere of responsibility.

Financial monitoring subjects use advanced information technology to monitor transactions and take preventive measures, such as building a customer profile following the results of investment testing in both traditional financial instruments and digital assets.

It is worth noting that the services are provided remotely, which reduces the risks of corruption between company employees and customers, as contact is eliminated; while at the same time to mitigate the risks of positive results of passing verification process by front men advanced mechanisms are introduced by financial monitoring subjects allowing for a relatively rapid but high quality “Know Your Customer” (KYC) process.

The company has established the “Three Lines of Defense” and “Four Eyes” principles, which aim to involve all employees in the process of combating money laundering and financing of terrorism and to mitigate the risk of errors due to human factor. However, it is not only consumers of financial services who may be involved in money laundering and financing of terrorism; the company therefore conducts due diligence on service providers and applicants for vacant positions within the company. Particular attention is paid to the assigned risk level of the provider in accordance with the Risk Management System of State Revenue Authorities.

Recognizing the social responsibility, novelty of technology, digital asset companies need to continue to provide awareness raising activities in the area aimed at improving financial and investment literacy.

They should regularly arrange podcasts, live broadcasts on the company's social media pages, and not forget to address the most vulnerable layers of the population: pupils, students and pensioners who, due to low financial literacy, may be involved in fraudulent and pyramid schemes.

It is critical to focus on developing the investor's own responsibility, fostering a culture of investing and developing rational and ‘saving’ behaviour aimed at accumulation, long-term planning and control of own finances, including digital assets.

Financial and tax advisers should be involved in the above work as only a comprehensive approach can bring fruitful results.

It is also of great importance to draw the attention of consumers of financial services to the fact that by investing through official platforms (crypto-brokers, crypto-exchanges) with an AIFC license, consumers will have an opportunity to apply to the AIFC Committee on Financial Services Regulation for protection of their rights, as well as receive relevant statements, and when applying to the accounting department, receive the necessary documents for timely and complete tax reporting of income obtained from digital asset value increase, which will further enable consumers to explain the sources of origin of income.

FROM INTELLECTUAL CONTESTS — TO NEW FINANCIAL SECURITY CHALLENGES

Ilya Yasinsky,
Director of the Financial Monitoring and Currency Control Department of the Bank of Russia

Ilya Yasinsky

Dear Readers,

Continuing the century-long traditions of the Olympiad movement, the current International Financial Security Olympiad serves as a kind of an intellectual contest platform for the most active and erudite representatives of the young generation.

Contest tests and competitive examinations envisaged by the program make you mobilize your skills and demonstrate your knowledge in a wide variety of fields and competences. I believe that participation in the Olympiad will serve as a good characteristic for a boy or girl's CV as they seek jobs in financial security sector, primarily in the anti-money-laundering system, both in public authorities and commercial and financial institutions.

The current financial security field is characterized by the dynamic and frequently unpredicted nature of its risk manifestations resulting from the prevention and combating of constant threat sources.

And, in this context, the AML/CFT/CPF system (anti-money laundering, counter financing of terrorism and counter financing of proliferation) plays a special role since it is focused on ensuring security of both individual states and their nationals in particular and the international community in general. The financial support of organized, including transnational, crime, has an adverse effect on the financial sector stability, as well as on the economic system of the states and endangers the wellbeing of many people.

One of the most important objectives of the Financial Monitoring and Currency Control Department of the Bank of Russia is to mitigate the risk of engagement of regulator-supervised entities in the conduct of suspicious transactions. Such transactions are made by unscrupulous entities to conceal the origin of sources and to further use their funds that are normally related to corruption, tax evasion, drug trafficking, terrorist group activities and other forms of organized crime.

Following the results of 2021, we note that the trend on decrease in number of such transactions in the bank sector is maintained. So, in comparison with 2020, the cash-out volume in the bank sector declined by 21% (from RUB 78 billion to RUB 62 billion); cash transfer volume on dubious grounds fell by 17% (from RUB 52 billion to RUB 43 billion); volume of sales with unreported third-party proceeds in the retail and travel sectors decreased by 16% (from RUB 36 billion to RUB 30 billion); volume of suspicious transactions dropped by 24% (from RUB 0.6 trillion to RUB 0.5 trillion).

However, the use of more sophisticated methods and advanced technologies in criminal activities assigns the task to AML/CFT specialists, including specialists of the Bank of Russia, related to continuous upgrade of professional competences and improvement of anti-money laundering measures.

One of the prospective developments of the Bank of Russia in this area is the “Know Your Client” (KYC) Platform information service. This service helps to ensure a required balance of anti-money laundering procedures in credit institutions so that, on the one hand, the trend on decrease in number of suspicious transactions is maintained and, on the other hand, an ecosystem of ‘green’ i.e. low-risk clients from a money-laundering and terrorist financing perspective is created thus providing a free payment flow for them.

Within the KYC Platform, the regulator will assess activities of legal entities and sole proprietors by classifying credit institution clients into three groups depending on the risk level: low (‘green’), medium (‘yellow’) and high (‘red’). Credit institutions should conduct the same work as well. Depending on the client risk degree (level), banks will determine an appropriate way of working with them.

The launch of the KYC Platform (from July 1, 2022) will reduce the burden on bona fide entrepreneurs, primarily on small and microbusiness, by decreasing the cost of interacting with credit institutions. The burden on credit institutions will be reduced as well. It will be possible by focusing their attention on transactions of clients of the higher (‘red’) risk. The last group includes clients that don’t conduct actual business activities, are registered in the name of front men, are controlled by third-party unscrupulous entities, complicate or make impossible the efforts made by tax and law enforcement authorities to identify suspicious transactions beneficiaries that facilitate payments in the shadow economy sector.

According to our estimates, low-risk clients account for 99% of the total number of business entities (currently around 7 million), and the number of high-risk clients does not exceed 0.7%.

Currently, the Bank of Russia jointly with the Federal Financial Monitoring Service conducts a large-scale ML/TF risk assessment campaign both at the national and sectoral levels. During this campaign, the main money laundering and terrorist financing ways and schemes, as well as their key factors have been systematized. Apart from that, development of tools for collecting and generalizing ML/TF expert risk assessment of various types of financial entities, services, and regions where such operations are performed has been completed. The ratings of the aforementioned risks provide the basis for improving the system of government and business measures to mitigate identified risks and vulnerabilities.

Apart from that, the level of ML/TF information and risk awareness should be raised for the business and individuals. This is contributed by training and contest activities for the youth similar to the current International Financial Security Olympiad.

Such events are aimed, alter alia, at enhancing financial and legal literacy of young people, as well as at demonstrating current economic security trends and new technological development areas in financial monitoring.

The ongoing escalation of geopolitical situation and the sanctions pressure increase give rise to new risks and financial security challenges for both the country as a whole, and for many industries, organizations and businesses and individual persons in particular. One of the main instruments of protection against these threats, which has already shown its effectiveness in the current conditions, has become a set of government measures in the field of currency regulation and currency control, which ensured the sustainability of our monetary unit as one of the foundations for the functioning of the entire economy.

These measures are not something entirely new to us. They have already been taken at the initial stages of the country's transition to market economy and have been gradually cancelled as things are turning towards making the ruble an international convertible currency and integrating the Russian financial system in the global system. In the current conditions, we were forced not only to restore a set of currency control measures in short time but also to adapt it to the new configuration of the domestic financial market and the system of its supervision by the Bank of Russia. In addition, we had to make adaptation to the existing types and tools of interaction between our financial market and the global one.

The readjustment process of the currency control system called for a significant mobilization of our resources and is not completed yet.

Therefore, we are setting an objective of creating a currency control system of a new type which is adaptable and flexible to changes and relevant factors. It is a great and exciting work requiring professional expertise, extensive knowledge, a fresh and creative view of daily life things, proactive and creative approach, as well as will and desire to achieve set goals. I am sure that the International Financial Security Olympiad participants, who possess these qualities, will make their input in this project.

I wish all participants would do their best in demonstrating their knowledge and skills. Be a success!

THE FIRST FINANCIAL SECURITY OLYMPIAD HAS SET A HIGH LEVEL OF ORGANIZATION

On March 15-16, 2022, the Conference of the International Network AML/CFT Institute (INI) on the topic "International Financial Security Olympiad: Experience and Goals for 2022" was held with the organizational and technical assistance of the ITMCFM via ZOOM videoconferencing

The Conference was attended by officers of Rosfinmonitoring, the Ministry of Science and Higher Education of Russia, the Ministry of Education of Russia, the International Training and Methodology Centre for Financial Monitoring, INI's member universities (21 Russian and 12 foreign universities) and financial intelligence units from Belarus, Kazakhstan, Kyrgyzstan, Tajikistan and Uzbekistan.

Welcoming speeches were delivered by **D. Afanasyev**, Deputy Minister of Science and Higher Education of Russia, **V. Glotov**, Deputy Director of Rosfinmonitoring, and **O. Koludarova**, Deputy Director of the Department of Upbringing, Supplementary Education and Children's Recreation of the Ministry of Education of Russia.

D. Afanasyev: – *We lay down the rules and traditions of the Financial Security Olympiad for years to come. Therefore, the key to success both last year and in the future, as it seems to me, is that this idea united a team of highly professional, interested colleagues representing financial intelligence practitioners, the university community and – now we can already say so – a team of participants and winners of the first Olympiad.*

V. Glotov: – *The initiative to expand the borders of the Olympiad movement and attract new participants was supported. Rosfinmonitoring has studied the issue of involving the Republic of Armenia and BRICS countries in our Olympiad movement. These countries supported the initiative of the Russian Federation, expressed their willingness to participate in the Olympiad and assured that they would assist their universities during the first and second stages of the Olympiad.*

O. Koludarova: – *The Financial Security Olympiad is one of the development vectors for the study of financial literacy and entrepreneurship basics among children. When we looked at last year's statistics, we saw that almost 1,400,000 pupils from over 19,000 schools took part in the All-Russian lesson on financial security. A good half of the schools in various regions of Russia responded to this initiative. This means that the topic is relevant and in demand, and we will continue to implement this event together in the future.*

The participants discussed the areas of preparation for delivering the "Financial Security" thematic lesson in 2022, holding the first and second stages of the International Financial Security Olympiad and conducting educational exhibitions of the International Network AML/CFT Institute in the EAG member states.

The ITMCFM representatives informed the Conference participants about the development of international scientific and educational digital platform "Sodruzhestvo" as well as about the plans to launch a series of educational exhibitions of the International Network AML/CFT Institute. The first exhibition was held as part of last year's final stage of the Sochi Olympiad; in 2022 its geographic scope has expanded significantly and now the exhibitions will be held in six countries participating in the Olympiad, namely, Belarus, Kazakhstan, Kyrgyzstan, Tajikistan, Turkmenistan and Uzbekistan.

M. Andronova, General Director of the ITMCFM:

– The first Financial Security Olympiad has set a high level of organization, and this year we would like to do better and to eliminate all the deficiencies of the last year, however insignificant and understandable they might be. We would be happy to increase the number of the Olympiad participants, and we welcome anyone who wants to join us. In this regard, we should pay particular attention to providing sufficient information to Russian and foreign students about the Olympiad, as well as to placing all necessary information on our resources.

V. Ovchinnikov, First Deputy General Director of the ITMCFM, Director of the International Network AML/CFT Institute:

– I would like to give credit to the heads and employees of our universities, Rosfinmonitoring Interregional Departments and financial intelligence units of the participating countries for the fact that last year everything was conducted in a very organized manner and within the prescribed time limits. That is why in 2022 each participating university will independently determine the organization policy of the qualifying stage and submit the lists of finalists agreed with Rosfinmonitoring Interregional Departments and financial intelligence units of the participating countries to the Olympiad Executive Committee.

THE FINANCIAL SECURITY OLYMPIAD – THE HUMAN RESOURCE POTENTIAL OF RUSSIA AND ITS PARTNER COUNTRIES

The 16th meeting of the International Network AML/CFT Institute's Council (INI) was held in Moscow

More than 100 representatives of research centers, INI's member universities, financial intelligence officers from Belarus, Kazakhstan, Kyrgyzstan, Russia, Tajikistan and Uzbekistan took part in the event in the face-to-face format, and representatives of China, Turkmenistan and a number of Russian universities – via videoconferencing.

The meeting was chaired by **Yury Chikhanchin**, Chairman of the INI Council and Director of Rosfinmonitoring. In his welcoming speech, the Head of the financial intelligence unit of Russia emphasized that the broad representation of participants once again demonstrates the integral connection between education, science and practice, while the issues under discussion require to consolidate the knowledge of the university and expert community.

The main issue of the Council meeting agenda was the second International Financial Security Olympiad. This year the Olympiad is divided into three events: the financial security lesson for pupils, the first and second stages of the Olympiad, and the development of the "Sodruzhestvo" digital platform, which in the future should unite pupils, students, teachers and members of the expert community around the Olympiad.

Yu. Chikhanchin: *"The Olympiad creates conditions for the organization of the international youth movement and community in the financial security sphere and unites pupils and students with professors and teachers of the International Network AML/CFT Institute, as well as with financial intelligence experts of Russia's partner countries in the international anti-money laundering system. The "Sodruzhestvo" digital platform is aimed at organizing the youth movement and expanding its geographic scope. It will make it possible to maintain communication in the period between the Olympiads, provide new knowledge and support each user."*

A. Lavrenko, Deputy Head of the Presidential Civil Service and Personnel Directorate, addressed the meeting participants with a welcoming speech.

A. Lavrenko: *"The International Network AML/CFT Institute has created an effective educational space in the Russian Federation and partner countries, ensuring the progressive development of the entire AML/CFT education system, allowing anti-money laundering specialists to interact and share information on a wide range of problems in this area, improve and enhance their professional level. The Olympiad becomes an important step in the successful development of the entire training system in the financial security sphere, laying a reliable foundation for the human resources potential of Russia and its partner countries in the international system."*

Director of the Department of State Policy and Management in the Sphere of General Education of the Ministry of Education **M. Kostenko** stated that today everyone needs financial education, and especially the younger generation:

M. Kostenko: *"The Ministry of Education always welcomes with great enthusiasm all the initiatives of Rosfinmonitoring in the sphere of education, and in particular the excellent experience of organizing the All-Russian thematic lesson on financial security. This year, all constituent entities of the Russian Federation received recommendations to deliver such lesson."*

Representatives of universities and research and educational centers that are members of the INI took part in the discussion of the agenda: General Director of the ITMCFM **M. Andronova,** Rector of the Peoples' Friendship University of Russia **O. Yastrebov,** Rector of the Siberian Federal University **M. Rumyantsev,** Rector of the Moscow Finance and Law University **A. Zabelin,** Rector of the National Research Nuclear University MEPhI **V. Shevchenko,** Rector of the Peter the Great St. Petersburg Polytechnic University **A. Rudskoy,** Vice Rector of the Plekhanov Russian University of Economics **A. Nikulin,** Director of the Training and Methodology Center of the State Financial Intelligence Service under the Ministry of Finance of the Kyrgyz Republic **L. Omurbekova,** Deputy General Director of the ITMCFM, Director of the International Network AML/CFT Institute **V. Ovchinnikov** and other participants of the meeting.

The Council decided to include new members in the INI, namely, Tajik National University, Kyrgyz State Technical University named after Iskhak Razzakov, Novosibirsk State Technical University, St. Petersburg State University of Economics and Southern Federal University (Rostov-on-Don, Russia).

PROMPT RESPONSE TO A CHANGING ENVIRONMENT

New money laundering and terrorist financing (ML/TF) risks emerge in our country in connection with the imposition of unilateral sanctions against the Russian Federation by unfriendly countries. This was the key topic at the March meeting of the Interagency AML/CFT/CPF Commission (IAC), which was held via videoconferencing

All the stakeholders of the Russian AML/CFT system continue to work in a planned manner to improve its effectiveness, including in the context of the Plan for Implementing the FATF Recommendations based on the results of 2019 assessment of Russia as far as it meets the national priorities of our country.

German Neglyad, State Secretary, Deputy Director of Rosfinmonitoring, emphasized that the work under the current circumstances continues both on the FATF platform and in the format of information interaction under the auspices of the Egmont Group of Financial Intelligence Units.

The key to effectiveness under the current conditions is the expansion of the financial monitoring scope, increasing the speed of information exchange on emerging risks, subsequent typologization of knowledge and conducting analysis for taking adequate response measures.

On March 16, 2022, the Bank of Russia and Rosfinmonitoring jointly issued and communicated to financial organizations an information letter on the need to increase attention to suspicious customer transactions due to the current situation. STRs will also be specially marked, which will improve the responsiveness to risks.

If such transactions are detected, credit institutions are advised to consider exercising their rights under Federal Law No. 115-FZ "On Combating Legalization (Laundering) of Proceeds of Crime and the Financing of Terrorism" with respect to such customer transactions.

Representatives of Rosfinmonitoring raised in their speeches the issues of improving the effectiveness of supervisory measures and private sector activities, as well as of terrorist financing classification taking into account the changed situation.

Yu. Chikhanchin

Today's meeting is taking place under difficult conditions, when unjustified unilateral sanctions have been imposed against the Russian Federation by a number of unfriendly countries, the reason for which became the special operation of the Russian armed forces in Ukraine. In order to stabilize the economy and the financial market, the President of the Russian Federation, the Government and the Central Bank of the Russian Federation have adopted and are implementing special economic measures. Significant extra funding is allocated to support the affected sectors of the economy, strategic companies and systemically important enterprises. All these circumstances indicate that new ML/TF risks arise in the changed conditions, which require assessment and taking measures. Our anti-money laundering system should rebuild itself and promptly respond to the changing situation.

NEWS BLOCK

MULTILATERAL INFORMATION EXCHANGE

In March 2022, the operational meeting of the Council of the Heads of Financial Intelligence Units of the CIS Member States (CIS CHFIUs) chaired by Rosfinmonitoring Director Yury Chikhanchin was held in virtual format via videoconferencing

The reason for the unscheduled meeting became the necessity of discussing new risks arising from the sanctions restrictions imposed against the Russian Federation in the context of the special military operation in Ukraine.

Taking part in the meeting were: Director of the Financial Monitoring Department under the National Bank of Tajikistan **Halim Mirsoaliev**, Head of the Department for Combating Economic Crimes under the General Prosecutor's Office of the Republic of Uzbekistan **Dilshod Rakhimov**, Chairman of the State Financial Intelligence Service under the Cabinet of Ministers of the Kyrgyz Republic **Kanatbek Turgunbekov**, Head of the Financial Monitoring Center of the Central Bank of the Republic of Armenia **Arakel Meliksetyan**, Chairman of the Financial Monitoring Agency of the Republic of Kazakhstan **Zhanat Elimanov**, and Director of the Financial Monitoring Department of the State Control Committee of the Republic of Belarus **Vyacheslav Reut**.

In his speech, Yury Chikhanchin reminded about considerable changes in the operational environment not only in the Russian Federation, but also in the entire CIS region which gave rise to new threats and risks. In these circumstances, the Russian FIU, being the national AML/CFT coordinator, still manages to successfully implement all planned activities despite the external political pressure.

In particular, Yury Chikhanchin informed the meeting participants about the attempt to exclude Russia from the Financial Action Task Force (FATF). In response, representatives of Rosfinmonitoring warned that such step could disrupt the balance in the global AML/CFT network and these considerations far outweighed the arguments of the opponents. After the decision of the Russian authorities to leave the Council of Europe, Russia also ceased to be a member of the Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL) – the European FSRB. However, Russia intends to continue its active work in the Eurasian Group on Combating Money Laundering and Financing of Terrorism (EAG), of which it currently holds the chairmanship.

The meeting participants reported about the operational environment in the CIS CHFIU member countries and exchanged views and opinions about the current situation. All FIUs confirmed their readiness to further coordinate their efforts and pursue joint activities.

Special attention was paid to development of the multilateral information interaction framework with the use of the Information Sharing System channels and the International Risk Assessment Center functionalities.

Head of Rosfinmonitoring Legal Department **Olga Tisen** reported about the legislative AML/CFT measures initiated following imposition of sanctions against the Russian Federation.

In his speech, Yury Chikhanchin reminded about considerable changes in the operational environment not only in the Russian Federation, but also in the entire CIS region which gave rise to new threats and risks. In these circumstances, the Russian FIU, being the national AML/CFT coordinator, still manages to successfully implement all planned activities despite the external political pressure.

COMBATING MONEY LAUNDERING AND TERRORIST FINANCING IS A PRIORITY FOR KYRGYZ REPUBLIC

A meeting of international donor organizations operating in the EAG region was held in Bishkek city (Kyrgyz Republic). Representatives of the International Training and Methodology Centre for Financial Monitoring (ITMCFM, Moscow, Russia) took part in the meeting

The purpose of the meeting was to coordinate the efforts of the partners in providing technical assistance to the Kyrgyz Republic, which in its turn should contribute to the country's progress in improving the national AML/CFT system. The event was arranged under the Technical Assistance Coordination Project for the Kyrgyz Republic which was launched in September 2021 and aimed at the practical implementation of one of the focus areas of the EAG Strategy 2019-2023.

In his welcoming speech, Mr. Adilet Dzhanuzakov, Director of the Situational Centre of the Presidential Administration of the Kyrgyz Republic noted that combating money laundering and terrorist financing is a priority for Kyrgyzstan.

Mr. Kanatbek Turgunbekov, Chairman of the State Financial Intelligence Service under the Ministry of Finance of the Kyrgyz Republic, Mr. Sergey Teterukov, Executive Secretary of the EAG, and Mr. Andrey Seleznev, Head of the Program Office of the United Nations Office on Drugs and Crime in the Kyrgyz Republic, also delivered the welcome speeches at the opening ceremony.

Representatives of the government authorities of the Kyrgyz Republic and representatives of the UN Counter-Terrorism Office, International Monetary Fund, International Training and Methodology Centre for Financial Monitoring of the Russian Federation, Organization for Security and Cooperation in Europe, United Nations Office on Drugs and Crime, US Embassy in Bishkek, Council of Europe, Financial Intelligence Unit of Iran and Financial Intelligence Unit of Serbia discussed ways and methods of ensuring technical assistance activities as provided for in the Project Plan developed by the EAG Secretariat.

The international meeting resulted in identification of donors that would provide technical assistance in the areas of highest priority for the country.

EURASIAN GROUP HIGH-LEVEL MISSION

Pursuant to the EAG Plenary decision, a high-level mission of the Eurasian Group on Combating Money Laundering and Financing of Terrorism (EAG) headed by the EAG Chairman, Director of Rosfinmonitoring, Yury Chikhanchin visited the capital of the Kyrgyz Republic, Bishkek city, on April 4, 2022

The Eurasian Group delegation also included Director of the Financial Monitoring Department of the State Control Committee of the Republic of Belarus Vyacheslav Reut, Chairman of the Financial Monitoring Agency of the Republic of Kazakhstan Zhanat Elimanov, and EAG Executive Secretary Sergey Teterukov.

The main goal of the mission was to discuss the capital amnesty program planned in the Kyrgyz Republic and further steps associated with this initiative, as well as to discuss a wider range of issues related to financial security of the country and the region as a whole.

In the course of the mission, the EAG delegation met with Chairman of the Cabinet of Ministers of the Kyrgyz Republic Akylbek Zhaparov who pointed out that the Kyrgyz Republic has always placed a great emphasis on the EAG mutual evaluations and technical assistance programs through which measures are being taken to improve the national AML/CFT system of the Kyrgyz Republic.

"*We have always felt the practical assistance of the EAG in creating and strengthening the legal and institutional framework for countering the financing of terrorism and money laundering. I would like to assure you that our Republic remains committed to complying with its international obligations. We intend to continue the course aimed at maintaining and developing our relations,*" - said Akylbek Zhaparov.

EAG Chairman Yury Chikhanchin informed the Kyrgyz Republic about the EAG procedures and further steps to be taken in respect of the capital amnesty program of the Kyrgyz Republic. He emphasized the need to initiate the preparation of the country for the 3rd round of the EAG mutual evaluations scheduled for 2025. He confirmed the readiness for further cooperation, including by providing expert and advisory support in the development of AML/CFT system, as well as in improving financial literacy among pupils and students of higher institutions as part of the Financial Security Olympiad planned for this year.

As part of the mission, a meeting was held with Chairman of the National Bank of the Kyrgyz Republic Kubahechbek Bokontayev, during which the issues of capital amnesty, regulation, supervision, assessment of risks associated with virtual assets, as well as other issues related to the regulation and supervision of the financial sector in Kyrgyzstan were discussed in detail.

The heads of the FIUs of the Republic of Belarus and the Republic of Kazakhstan shared their valuable experience and useful practical information on the issues under consideration.

At the end of the mission, the EAG delegation visited the State Financial Intelligence Service under the Ministry of Finance of the Kyrgyz Republic and got acquainted with the activities of its departments, including its Training and Methodology Center.

NETWORK INSTITUTE IS AN IDEA GENERATION PLATFORM FOR TRAINING OF AML/CFT SPECIALISTS

The International Network AML/CFT Institute (INI) Conference entitled "Target Integration Model of AML/CFT Training Courses in Educational Process" was held in Moscow

The Conference was opened by the ITMCFM General Director Margarita Andronova:

— I would like to thank our colleagues from Belarus, Kazakhstan, Kyrgyzstan, Russia, Tajikistan and Uzbekistan for finding an opportunity to attend this event. Hopefully, our joint efforts will result in adoption of a unified list of competencies for training the AML/CFT specialists and also in development of a list of AML/CFT training courses that could be incorporated into the educational programs of the INI's member universities.

The key topic of the first day of the Conference was the "Developing and Updating AML/CFT Educational Programs and Training and Methodological Materials". After that, the three groups composed of the Conference participants were set up to discuss the following topics: "Law and International Relations", "Economics and Finance" and "Information Technologies".

The final session was devoted to summing up the results. The members of the groups delivered presentations on integration of AML/CFT training courses into the educational programs and answered the questions of the colleagues.

Summarizing the key outcomes, Conference moderator **S. Zinkovsky** (Project Manager of the ITMCFM Research and Educational Projects Coordination Department) pointed out that the Conference demonstrated that the International Network AML/CFT Institute has become the platform that enables consideration and discussion of various ideas related to training of AML/CFT specialists under different educational programs.

M. Andronova

I would like to thank our colleagues from Belarus, Kazakhstan, Kyrgyzstan, Russia, Tajikistan and Uzbekistan for finding an opportunity to attend this event. Hopefully, our joint efforts will result in adoption of a unified list of competencies for training the AML/CFT specialists and also in development of a list of AML/CFT training courses that could be incorporated into the educational programs of the INI's member universities.

PROFESSIONAL DEVELOPMENT TRAINING OF TEACHING STAFF

In parallel, a traditional professional development training course "AML/CFT Financial Investigations: Analyst's Tools" was delivered to teaching staff of the INI's member universities.

In their welcome speeches to the participants, ITMCFM First Deputy General Director, Director of INI **Vladimir Ovchinnikov**, as well as ITMCFM Deputy General Director, Head of the ITMCFM Research and Educational Projects Coordination Department **Irina Shilina** summarized the practices of professional development training over the previous years and outlined the objectives of the INI's member universities in the current year.

The first day of the training course was devoted to financial investigations and AML/CFT analytical activities. The subsequent training sessions were arranged in form of lectures, roundtables, practical workshops and joint and individual practical exercises.

WE HOPE TO MAINTAIN AND STRENGTHEN OUR ALLIANCE!

The Tenth Anniversary of the Training and Methodology Center of the State Financial Intelligence Service under the Ministry of Finance of the Kyrgyz Republic

Dear Mrs. Omurbekova!

Dear Colleagues!

Since its establishment, the Training and Methodology Center (TMC) of the State Financial Intelligence Service (SFIS) has proved to be an important and reliable partner of the International Training and Methodology Centre for Financial Monitoring (ITMCFM). In cooperation with the financial intelligence units of the EAG countries and the member universities of the International Network AML/CFT Institute (INI), we pursue meaningful and fruitful cooperation for strengthening the capacity of the national AML/CFT systems of the Eurasian region countries.

Satisfying the staffing needs of the financial intelligence units of the Kyrgyz Republic and the Russian Federation has always been and remains one of the key priorities of our Centers. Implementation of joint educational projects allows us to develop unified approaches to training of highly demanded AML/CFT specialists, ensure high quality of practice-oriented training of specialists taking into account the national specificities of individual countries in the Eurasian region context, and develop new forms of interaction among the AML/CFT research and educational institutions.

In 2013, the financial intelligence unit of Kyrgyzstan was one of the first agencies that recommended Kyrgyz universities for incorporation into the International Network AML/CFT Institute and assisted in professional orientation of students for enrollment in the Russian universities under the AML/CFT educational programs. The financial monitoring educational program for the Kyrgyz Republic was developed by the Kyrgyz-Russian Slavic University in close coordination with the Training and Methodology Center of the State Financial Intelligence Service. Every year, dozens of applicants from the Kyrgyz Republic are provided with the opportunity to enter the Russian universities with the support of our Training and Methodology Centers on a free-of-charge basis.

It should also be noted that the TMC specialists provide ongoing practical support to the students from the Kyrgyz Republic by holding meetings with them and participating in presentation of their graduate projects. Furthermore, with the support of the FIU and TMC of the Kyrgyz Republic, the Kyrgyz students delivered presentations on the margins of the Eurasian Group plenary meetings. Three years ago, the TMC held, with the support of the ITMCFM and the Embassy of the Kyrgyz Republic in the Russian Federation, the meeting with the Kyrgyz students studying in Moscow universities to discuss issues most relevant for students related to education, employment, research and practical activities. All this demonstrates the keen interest and engagement of the TMC in training of AML/CFT specialists.

In 2020, the TMC created the student council composed of scholarship holders who enroll and study in the Russian member universities of the International Network AML/CFT Institute under the quotas granted by Rosfinmonitoring. The student

council was established primarily for consolidation of the INI student community, creation of a student information environment, participation in events arranged by the TMC, cooperation with different public associations and institutions for holding joint events, etc.

In 2021, the first International Financial Security Olympiad was held in the Eurasian region. Being one of the coordinators of this event, the ITMCFM had the opportunity to ensure the professional approach of our colleagues from the TMC to arrangement of the qualifying stage of the Olympiad in cooperation with the FIU of the Kyrgyz Republic and member universities of the International Network AML/CFT Institute. The TMC became the main platform for coordinating this work and selecting nine finalists who came to "Sirius" educational center (Sochi city) in autumn to participate in the final stage of the Olympiad. The Kyrgyz students demonstrated excellent knowledge and skills and won one of the prizes.

In 2018, with a view to creating a unified AML/CFT educational space, the ITMCFM implemented, in cooperation with the Kyrgyz Republic, a series of educational projects within the framework of providing technical assistance to the Eurasian region countries. One of these projects involved the development of a basic training manual "Specificities of the National AML/CFT Systems of the Eurasian Region Countries", the second volume of which devoted to the national AML/CFT system of Kyrgyzstan was published in 2019. This volume was drawn up by an author team composed of specialists of the Training and Methodology Center of the State Financial Intelligence Service of the Republic of Kyrgyzstan, the Kyrgyz-Russian Slavic University and the International Training and Methodology Centre for Financial Monitoring. This training manual proved to be highly demanded not only by the Kyrgyz universities, but also by other universities of the EAG countries where the Kyrgyz students undergo training. We are very glad that our joint research efforts yielded such a positive result.

Over the past ten years, our Centers have interacted and cooperated at many international platforms, such as the EAG plenary meetings, workshops, forums, international conferences and the INI board meetings held in both virtual and face-to-face formats. The ITMCFM specialists regularly participate in the events arranged on the territory of the Kyrgyz Republic with the support of the TMC of the Republic of Kyrgyzstan. Such events were often held at the city of Cholpon-Ata near the Issyk-Kul Lake. In particular, in September 2019, it hosted the Eurasian AML/CFT Forum arranged under the auspices of the Kyrgyz State Financial Intelligence Service and its Training and Methodology Center, where we shared the expert opinions and informed the participants about recent achievements in the ML/TF investigation practices. A month before that, the workshop on effective use by financial institutions of the international AML/CFT standards related to application of a risk-based approach was arranged and held jointly by the TMC and ITMCFM. The workshop goal was to inform about ML/TF sectoral risk assessment methodology

and to share experience of conducting ML/TF risk assessment and implementing risk-based approach by private sector entities.

In the last two years, the COVID-19 pandemic made significant adjustments in the organization of face-to-face events, but it did not prevent us from continuing our productive work and cooperation in virtual format. Our experts held videoconferencing sessions to share modern methodological approaches to addressing the specific risks and threats. In 2020, the ITMCFM arranged, in cooperation with Rosfinmonitoring, the State Financial Intelligence Service of the Republic of Kyrgyzstan and the SFIS Training and Methodology Center, a series of thematic workshops on national risk assessment for the members of the SFIS Working Group on organizing and conducting the NRA.

Summarizing the results of our fruitful cooperation over the past ten years, it can be stated that the TMC and the ITMCFM have worked and continue to work for enhancing the capacity of the financial intelligence units, law enforcement agencies, judicial and prosecution authorities, national security agencies, oversight and obliged entities by conducting high quality professional training of officers in charge as part of our unified strategy aimed at strengthening of human resource and professional capacity of the national AML/CFT systems of the Russian Federation and the Kyrgyz Republic.

We congratulate all personnel of the Training and Methodology Center of the State Financial Intelligence Service under the Ministry of Finance of the Kyrgyz Republic on the 10th anniversary of the establishment of the Center and wish them good health, well-being and further achievements. We hope to maintain and strengthen our alliance for ensuring financial security of our countries and the Eurasian region as a whole!

We congratulate all personnel of the Training and Methodology Center of the State Financial Intelligence Service under the Ministry of Finance of the Kyrgyz Republic on the 10th anniversary of the establishment of the Center!

ITMCFM Team

36th EAG PLENARY MEETING IN UZBEKISTAN – FIRST PLENARY HELD IN HYBRID MODE SINCE 2019

The 36th Plenary Meeting of the Eurasian Group on Combating Money Laundering and Financing of Terrorism (EAG) was held in Tashkent (Republic of Uzbekistan) from May 30 to June 2, 2022.

In view of the difficult global epidemiological situation, the recent EAG Plenary Meetings were held in virtual format via videoconferencing. The 36th Plenary in Tashkent (Republic of Uzbekistan) is the first meeting physically attended by most delegations from the EAG member states and international organizations over the last two years.

It was underlined in the opening remarks of the EAG Chairman and Director of Rosfinmonitoring Yury Chikhanchin: "Dear colleagues and friends! After more than a two year period when we could not meet in person, I am very pleased to see all of you in good health and excellent mood in the sunny and

hospitable Tashkent. I sincerely thank all colleagues and the authorities of the Republic of Uzbekistan for perfect organization of the plenary session, as we all know how much effort and resources it required. It is particularly impressive that these plenary arrangements were made in parallel with the ongoing mutual evaluation. Unfortunately not all delegations were able to physically attend our plenary meeting despite the obvious decline in the COVID-19 pandemic. I would like to extend a special welcome to the Chinese colleagues and other attendees who joined us, albeit in virtual format. Nevertheless, we hope that the overall COVID-19 situation will improve soon, so that all delegations will be able to physically participate in the next Plenary."

In his welcome speech to the Plenary, Deputy Prime Minister, Minister of Economic Development and Poverty Reduction of the Republic of Uzbekistan Jamshid Kuchkarov emphasized the need for well-established and coordinated joint efforts: "The Eurasian Group on Combating Money Laundering and Financing of Terrorism plays an important role in strengthening economic security and ensuring effective coordination and cooperation among its member states. Legalization of criminal proceeds is currently one of the main challenges for many countries. Emergence of new threats and vulnerabilities requires implementation of more effective coordination mechanisms at both national and international levels. Today, we gathered together to share views and opinions about measures taken in this regard and to develop recommendations for further improvement of our joint efforts in this area".

The Plenary Meeting was attended by the delegations of the EAG member states: Belarus, India, Kazakhstan, China, Kyrgyzstan, Russia, Tajikistan, Turkmenistan and Uzbekistan, as well as by representatives of the EAG observer countries and organizations: Iran, South Korea, Mongolia, Serbia, USA, FATF, Council of Europe Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL), CIS Anti-Terrorism Center, UN Office on Drugs and Crime (UNODC), Organization for Security and Cooperation in Europe (OSCE) and Shanghai Cooperation Organization (SCO). Deputy Prime Minister for Financial and Economic Affairs and Poverty Reduction, Minister of Economic Development and Poverty Reduction of the Republic of Uzbekistan Jamshid Kuchkarov, Deputy Chairman of the Federation Council of the Federal Assembly of the Russian Federation Nikolai Zhuravlev, and Chairman of the Committee of the Senate of the Oliy Majlis of the Republic of Uzbekistan Nariman Umarov addressed the Plenary with welcome speeches.

The Plenary session agenda included meetings of the Working Groups and the EAG Plenary Meeting, the International Scientific and Practical Conference "Legalization of Proceeds from Crime and Terrorism Financing: Current Threats and Challenges to Address them" and the 19th Meeting of the Council of the Heads of Financial Intelligence Units of the CIS Member States (CIS CHFIUs).

One of the key topics of the Plenary Meeting agenda was the adoption of the Mutual Evaluation Report of the Republic of Uzbekistan. After considering and discussing the MER, the delegations recognized the AML/CFT system of the Republic of Uzbekistan as one of the best in the region.

Besides that, the Protocol amending the Agreement on the EAG and the Regulation on the Procedure for Forming and Executing the Budget of the EAG was signed by the member states. Entry into force of these documents will provide for further development of cooperation and will extend the range of instruments required for accomplishing the EAG goals and objectives. The introduced amendments are aimed at updating the basic concepts (terms) in line with the current FATF international standards.

The Plenary positively appreciated the efforts of the International Training and Methodology Centre for Financial Monitoring (ITMCFM) in terms of implementation of educational and technical assistance projects. In her presentation, Head of the ITMCFM Organization and Information Support Department Ludmila Stepanova suggested creating an Association of the EAG Training and Methodology Centers. This initiative was supported and approved by the Plenary.

The Plenary heard the report on preparing and conducting the annual International Financial Security Olympiad. This year, pupils and students from Russia, the EAG member states and the BRICS member countries will take part in the qualifying stage of the Olympiad. The Olympiad final stage will be held in “Sirius” federal territory on October 10-14, 2022.

At the end of the plenary session, the results of the 8th Best Cooperation Contest were announced. The Zubkov prize was awarded to the Contest winner – the Republic of Uzbekistan.

EAG Chairman Yury Chikhanchin noted the excellent arrangement of the 36th Plenary Session and expressed, on behalf of the delegations, gratitude to all parties who organized this event.

The 37th EAG Plenary Meeting will be held in the Republic of Tajikistan in November 2022.

Subscribe to Telegram channels of Rosfinmonitoring and the ITMCFM

Publisher

Autonomous Non-Profit Organization ITMCFM
Staromonetny Lane 31, bld.1,
Moscow, Russia, 119017. E-mail: info@mumcfm.ru.

Autonomous Non-Profit Organization ITMCFM

2022