R. ARTYUKHIN

"Identification and prevention of risks of failure to achieve due results related to the national projects are one of the priorities of Rosfinmonitoring and the Federal Treasury".

CONTENTS

EDITORIAL BOARD

Chairman of Editorial Board

Yury Chikhanchin

Deputy Chairman of Editorial Board

Vladimir Ovchinnikov

Editor in Chief

Irina Ivanova

Members of Editorial Board

Yury Korotkiy

Galina Bobrysheva

Vladimir Glotov

Oleg Krylov

Alexander Klimenchenok

Evgeny Legostaev

Sergey Teterukov

Alexey Petrenko

Evgeny Mozgov

German Neglyad

DEAR READERS,

Year 2020 brings us a new set of challenges. Assessing the previous year's outcomes and the hard work of all AML/CFT system stakeholders that preceded it, we should draw conclusions and coordinate actions to improve the effectiveness of overall AML/CFT/CPF framework.

Recent evaluation has underscored the ability of government agencies and the private sector to work together towards a common goal. Today our priority lies in improving the mechanism aimed at application of a risk-based approach to supervisory activities; facilitating the adoption of systemic solutions at the country level during the investigation of money laundering, including using international shadowy platforms; developing mechanisms for the search and recovery of assets; decriminalizing the economy; preventing and suppressing misuse of budgetary funds. Challenges related to countering terrorism, elimination of terrorist financing channels and supply of weapons still remain relevant.

In conclusion, I would like to quote the President of the Russian Federation Vladimir Putin, who, speaking at the Federal Security Service Collegium, set a goal for all of us:

"I've already spoken about this many times and I want to repeat it once again: we allocate huge resources to achieve goals of national development, and these efforts should be result-oriented. The success of these efforts depends to a great extent on you too."

Yury Chikhanchin
Director of Rosfinmonitoring

ROLE OF FEDERAL TREASURY IN ENSURING TRACEABILITY OF NATIONAL PROJECTS IMPLEMENTATION PROGRESS

In the modern context, the effective public governance involves timely monitoring of global challenges and development of innovative response measures

Roman Artyukhin,
Head of the Federal Treasury of the Russian Federation

Roman Artyukhin

The financial and budgetary system of the Russian Federation, being the essential element of the State, should be able to maintain stability and appropriate balance of budget resources and, at the same time, ensure highly efficient performance of the government functions.

The national projects, developed pursuant to the Decree of the President of the Russian Federation Vladimir Putin *on National Goals and Strategic Objectives of Development of the Russian Federation until 2024*, are the breakthrough mechanism that promotes research and technological advancement, as well as social and economic development of the country, facilitates the rise in the living standards and creates conditions and opportunities for developing talents and full potential of each individual.

At present, the so-called "project-based approach", which is aimed at achieving the specific goals and results, is being implemented on the nationwide scale.

The preparatory work conducted in the middle of last year included development of the regulatory and methodological frameworks and launch of the interaction mechanisms among the government authorities, business communities and general public. These efforts required the fundamental changes in the operation of the government agencies as well as introduction of modern approaches at all levels of public governance. It is the constituent regions of the Russian Federation where most of the national projects-related tasks are fulfilled.

The first year of implementation of the national projects demonstrated the need for further improvement of the regulations in order, among other things, to avoid duplication of information contained in the submitted reporting documents and to ensure end-to end oversight of budget expenditures, along with reduction of administrative burden borne by project contractors. It is necessary to refine the government mechanisms and suggest convenient and effective solutions to the contractors so that they can work without falling behind the schedule.

One of the goals of the national projects involves not only proper disbursement of the public funds, but also effective and targeted use of these funds. However, it should be noted that the general public not always can feel and trace the results of implementation of the national projects, including the situations where these results have been actually achieved.
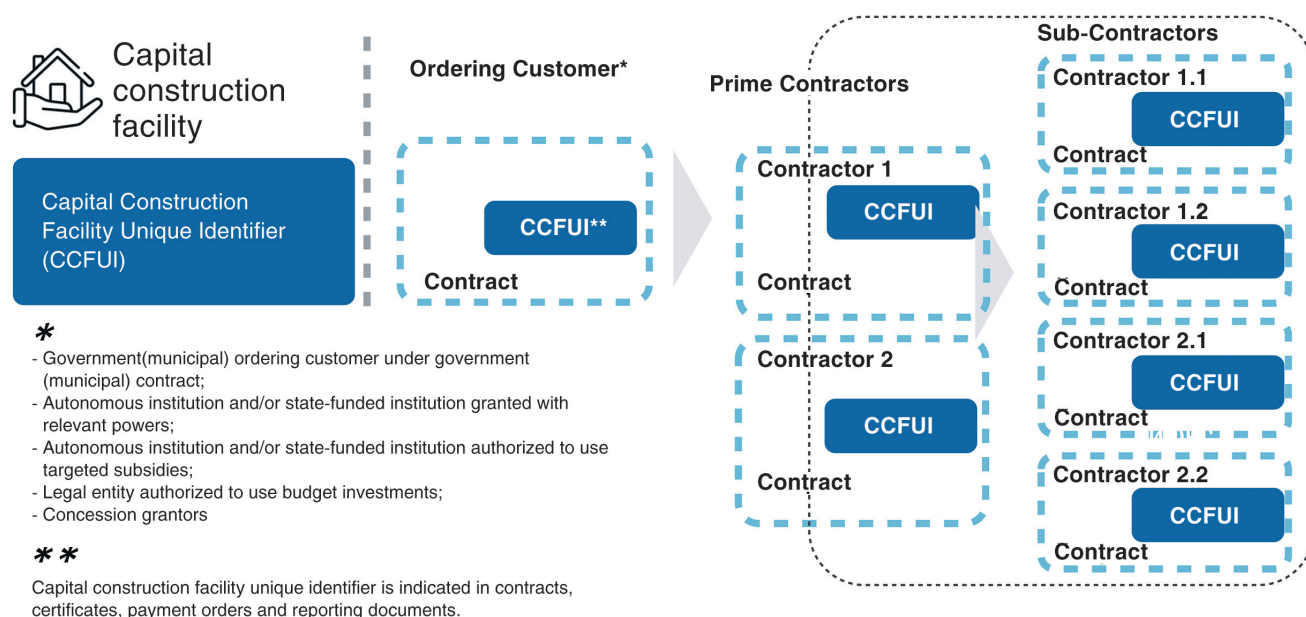
The Government Project Office of the Russian Federation, Ministry of Finance, Federal Treasury and Federal Financial Monitoring Service actively work to develop the "traceability" model that would allow to trace reaching of milestones and outcomes of the federal and regional projects.

This national project milestones and results traceability model under development is built on the principles of cascading the information from general data down to information on specific result.

Information on implementation of the national projects is represented through the application of the infographics tools and is posted on the map of the Russian Federation. The subsystems of the *Electronic Budget* State Integrated Public Funds Management Information System are used as the information sources.

At present, the pages layouts visualizing the information on implementation of the national projects (based on the example of the capital construction facilities) have been designed and posted on the Unified Portal of the *Electronic Budget* State Integrated Information System.

Scheme: Application of Capital Construction Facility Unique Identifier

Capital construction facility

Capital Construction Facility Unique Identifier (CCFUI)

Ordering Customer*

CCFUI**

Contract

Prime Contractors

Contractor 1

CCFUI

Contract

Contractor 2

CCFUI

Contract

Sub-Contractors

Contractor 1.1

CCFUI

Contract

Contractor 1.2

CCFUI

Contract

Contractor 2.1

CCFUI

Contract

Contractor 2.2

CCFUI

Contract

*
- Government(municipal) ordering customer under government (municipal) contract;
- Autonomous institution and/or state-funded institution granted with relevant powers;
- Autonomous institution and/or state-funded institution authorized to use targeted subsidies;
- Legal entity authorized to use budget investments;
- Concession grantors

**
Capital construction facility unique identifier is indicated in contracts, certificates, payment orders and reporting documents.

Thus, a person residing in any region of the Russian Federation can see what particular facilities are created in the framework of the national projects in the respective region.

It is critically important to ensure maximum transparency and accessibility of information on progress in implementation of the national projects for their successful completion. A unique result identifier of a given project may be used as the effective monitoring tool applied at all project stages - from the initial planning to ultimate completion. The unique result identifier should be indicated not only in the project profiles and government (municipal) contracts, but also in all settlement and payment documents, *inter alia*, at all levels of cooperation of the prime contractors under the government (municipal) contracts.

For example, it is necessary to sign a number of government (municipal) contracts at certain stages of creating capital construction facility, e.g.: to carry out expert reviews, conduct building and assembly work, procure and install equipment, etc. Failure to meet the terms of any of these contracts may result in untimely commissioning of the facility and jeopardize implementation of the entire national project. It is this unique result identifier that allows for linking government (municipal) contracts to particular facility.

The Federal Treasury of the Russian Federation uses similar instrument for carrying out treasury supervision of individual government contracts.

Identification and prevention of risks of failure to achieve the results related to the national projects at all stages of their implementation are one of the priorities of Rosfinmonitoring and the Federal Treasury. The refined interagency information sharing mechanism allowes not just to identify unscrupulous contractors, but also to create risk profiles of individual projects. For this purpose, it is very important to ensure that information on such risks is timely communicated to responsible contractors, plenipotentiary representatives of the President of the Russian Federation in the Federal Districts, governors, project offices and other government stakeholders.

At the meeting of the members of the Sub-Group on Coordination of Supervision and Oversight Activity held on October 7, 2019 the Interagency Working Group on Monitoring and Overseeing Effectiveness of Implementation of National and Federal Projects of the Bureau of the Strategic Development and National Projects Council under the President of the Russian Federation decided to develop a methodological approach to monitoring the results of the national projects and assessing risks related to implementation of government (municipal) contracts.

It is planned that the relevant functions will be implemented in the automated information system, which is currently under development. This system will allow to:

- Trace funding of the national, federal and regional projects (including targeted funds allocated from the federal budget);

- Monitor current situation on performance of the government (municipal) contracts as part of the implementation of national projects;

- Assess risks of failure by contractors to fulfill their obligations under the government (municipal) contracts;

- Enhance reliability of reported data on the achieved results provided by the government authorities by using the independent assessment tools, including publication of data in the publicly accessible sections of the information system.

It is important to see the overall picture of implementation of the national projects at all levels of the budgetary system of the Russian Federation and to perform operative online monitoring of the ongoing events. This can be achieved through the application of the information and analytical system that monitors implementation of the national projects and integrates data of almost all government agencies. It will allow to assess risks and warn about deviations from the achievement of the national project objectives and target indicators.

Creation of a unified information resource that will provide for integration with the information systems of various government authorities will make it possible to significantly simplify information sharing process among different oversight authorities and will allow to plan and conduct monitoring activities with the application of the risk-based approach.

The oversight and supervisory authorities will be able to move towards combined format of monitoring and supervisory activities (which includes both off-site and on-site inspections), conduct remote analysis of the supervised entities and coordinate their activities in order to avoid duplication of efforts. On-site inspections will be conducted only when off-site inspections identify risks of failure to achieve the milestones of the national projects' outcomes.

The efforts pursued by the Federal Treasury in the capacity of the national budget and financial supervisor, which involve digitization of data, extensive application of information technologies, alignment of methodologies and risk management systems with other oversight authorities and interagency information sharing, will allow to adequately monitor achievement of the national projects objectives in a cost-effective manner. Such approach is deemed consistent with the national goals of the state sustainable development.

CHALLENGES ASSOCIATED WITH IDENTIFICATION, ASSESSMENT AND MITIGATION OF RISKS IN BUDGETARY SPHERE

In recent years a number of critically important tasks related to ensuring the safety of the public funds spending have been assigned to Rosfinmonitoring by the national government

Mikhail Sedov,
Head of the Department on work with the Public Sector
Federal Financial Monitoring Service

Since 2015, Rosfinmonitoring has been a member of the interagency system aimed at monitoring appropriate spending of public funds allocated for the implementation of the defence procurement. Since 2017, as part of the gradual transition to treasury supervision of budgetary funds, Rosfinmonitoring has become a stakeholder of the budget monitoring and treasury supervision system.

Main Work Streams

- Defence procurement

- Public procurement

- Monitoring of the national and federal projects implementation

- Monitoring of strategic associations

- Financial stability of the defence industry enterprises

The efforts that have been pursued on an ongoing basis include monitoring of operation of the systemically and strategically important companies, ultimate recipients of government subsidies allocated for supporting the agricultural and forestry sectors as well as monitoring of operation of the defence industry enterprises – in terms of identification of risks affecting their financial sustainability.

DEFENCE PROCUREMENT

In order to detect and assess risks that may occur as a result of transactions with funds or other assets carried out in the course of implementation of the defence procurement contracts, nearly 3.3 thousand business entities were subject to inspections and audits in 2019. Based on the findings of these inspections, 404 case materials concerning the audited entities were sent to the members of the interagency monitoring system as well as to the law enforcement agencies and prosecution authorities. The total number of case materials submitted in 2019 increased by 22% compared to 2018.

The main identified risks are related to the use of shell resident legal entities (shell companies) as well as to suspicious financial transactions carried out for "cashing out" of public funds.
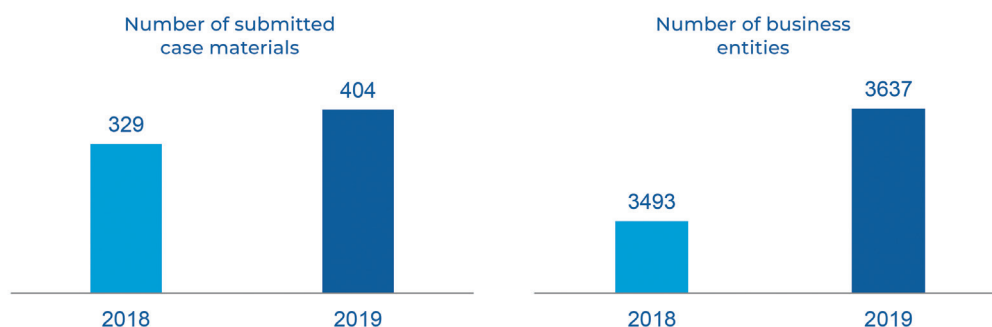
As a result of the response measures taken in coordination with the members of the interagency defence procurement monitoring system, the law enforcement agencies and prosecution authorities terminated a number of contracts, which allowed to prevent embezzlement of a total of RUR 2.8 billion allocated under the defence procurement contracts.

The undertaken measures also led to successful recovery back to the federal budget of over RUR 5.4 billion that have been earlier paid as advance payments to unscrupulous contractors.

In general, the results achieved in 2019 as part of the interagency defence procurement monitoring system are indicative of decriminalization of the sector and enhancement of transparency of payments and settlements, in particular:

- Number of contractors involved in suspicious transactions declined by 20%, and amount of such transactions decreased more than threefold;

- Number of contractors suspected of being fictitious reduced by over 30%;

- Amount of rejected transactions that have no economic rationale decreased by 41%.

Defence Procurement

Number of submitted case materials: 2018: 329, 2019: 404

Number of business entities: 2018: 3493, 2019: 3637

Main Identified Risks

- Risks related to the use of shell resident legal entities (shell companies)

- Risks related to suspicious financial transactions carried out for "cashing out" of public funds

At the same time, it is noted that corruption-related risks still remain high. Instances of payment for non-completed work, misuse of public funds for purposes inconsistent with the terms of their allocation, payment of salary in excess of the established rates, etc. are still detected. All this requires additional response measures to be taken by the prosecution, oversight and supervisory authorities, Rosfinmonitoring and other government agencies.

NATIONAL AND FEDERAL PROJECTS

Since 2019, Rosfinmonitoring has been involved in overseeing and monitoring the effectiveness of implementation of the national and federal projects.

In 2019, a total amount of funds allocated for implementation of the national projects and the comprehensive plan of upgrading and expanding the trunk infrastructure from all financing sources exceeded RUR 3 trillion, approximately 80% of which were provided from the federal budget and consolidated regional budgets.

Monitoring of appropriate spending of the public funds (budget obligation limits, cash expenditure) allocated for implementation of the national and federal projects revealed the risks that are unusual for the money laundering schemes used in budget sphere and are caused by ineffective management system related to delays in transferring funds to the government customers and consequently results in intensified contracting procedures at the end of a year. All this may affect timely achievement of the milestones and have negative impact on quality of the national and federal projects results.

At the same time, the existing structure of the targeted expenditure items applicable to the national projects allows for "highlighting" the portion of funds allocated from the federal budget for the indicated purposes. For example, there are problems related to monitoring the disbursement of the federal budget funds allocated as subsidies to the constituent regions of the Russian Federation that do not use the treasury system for cash execution of the budget. There are also problems with "highlighting" funds allocated for implementation of the projects from the regional budgets and extra-budgetary funds raised for implementation of the national and federal projects.

Results of Defence Procurement Monitoring

RESULTS
₽

RUR 2.8 billion was saved from misappropriation as a result of termination of contracts

Public funds in amount of over 5.4 billion were recovered

105 criminal proceedings were initiated as a result of inflicted losses amounting to over RUR 4 billion

Over 164 notifications to rectify the identified breaches of the legislation were issued

68 executive officers were held administratively liable

Tax inspections were organized in 230 business entities that were not physically present at the addresses of their government registration or were established using straw men

National and Federal Projects

Funding allocated for 2019

- RUR 1,779 billion (58.2%) – federal budget
- RUR 614.5 billion (20%) – consolidated regional budgets
- RUR 667.7 billion (21.8%) – non-budgetary sources

Identified Risks

- Ineffective management
- Use of resident shell legal entities (shell companies)
- Suspicious financial transactions carried out for "cashing out" of public funds

Challenges

- Public funds allocated as subsidies to the constituent regions of the Russian Federation that do not use the treasury system for cash execution of the budget are not subject to monitoring
- Extra-budgetary funds raised for implementation of the national and federal projects are not subject to monitoring

Results of National Projects Monitoring
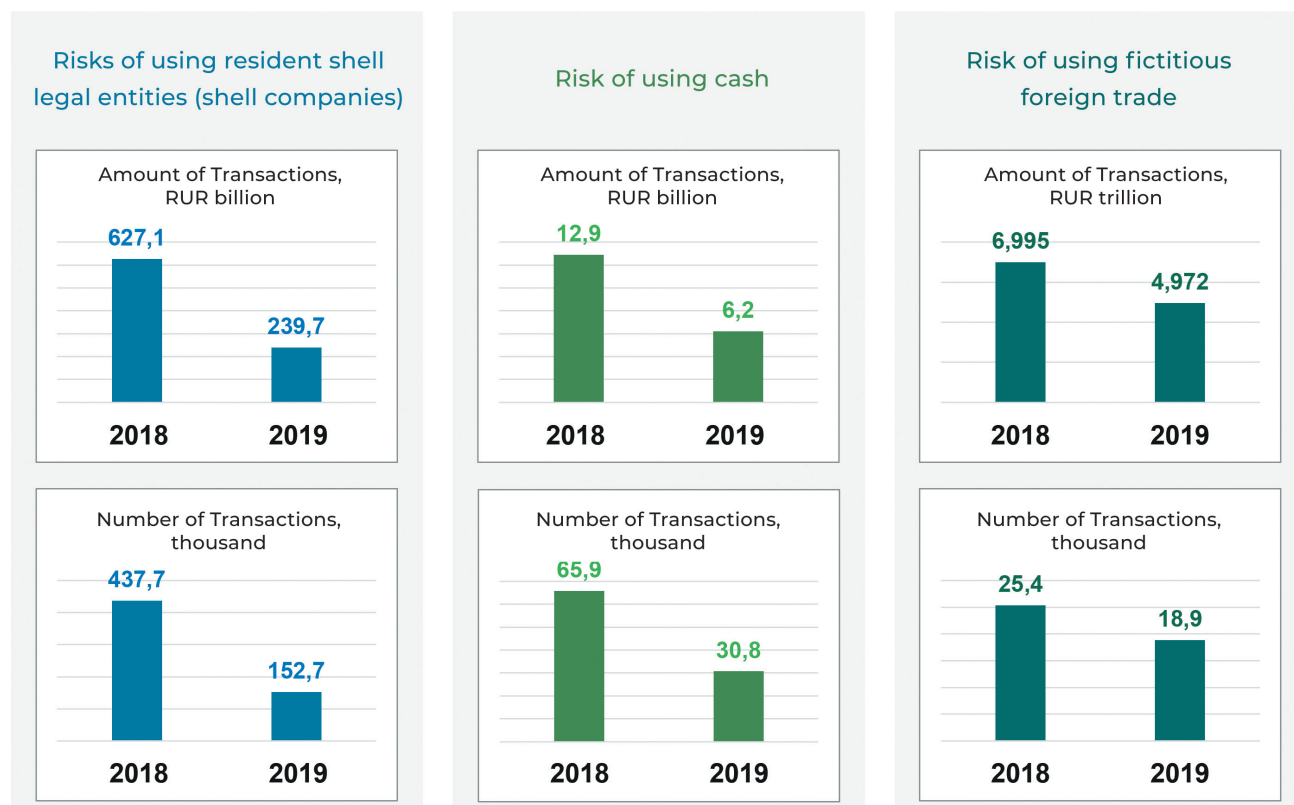
RESULTS
₽

Collusive bidding schemes amounting to nearly RUR 5.5 billion were revealed in cooperation with the Federal Antimonopoly Service

Procurements amounting to over RUR 450 million were cancelled

Contracts amounting to more than RUR 660 million were terminated

13 criminal proceedings were initiated as a result of inflicted losses amounting to over RUR 1.76 billion

Effectiveness of Efforts Undertaken for Mitigating ML Risks in Budgetary Sphere

Risks of using resident shell legal entities (shell companies)

Amount of Transactions, RUR billion

627,1 — 2018
239,7 — 2019

Number of Transactions, thousand

437,7 — 2018
152,7 — 2019

Risk of using cash

Amount of Transactions, RUR billion

12,9 — 2018
6,2 — 2019

Number of Transactions, thousand

65,9 — 2018
30,8 — 2019

Risk of using fictitious foreign trade

Amount of Transactions, RUR trillion

6,995 — 2018
4,972 — 2019

Number of Transactions, thousand

25,4 — 2018
18,9 — 2019

To address the aforementioned problems, it is necessary to implement elements of treasury or banking supervision and introduce a unified public contract identifier similar to that used in defence procurement.

Currently, these and other initiatives are being explored and considered in coordination with the Federal Treasury, which includes the development of the layout system for monitoring achievement of the national projects results to be integrated in the *Management* State Automated Information System.

In 2019, based on the risks related to the use of shell companies and associated with suspicious financial transactions carried out for "cashing out" of public funds identified by Rosfinmonitoring, 740 case materials concerning over 4.3 thousand business entities were submitted to the oversight, supervisory authorities and law enforcement agencies. The total amount of suspicious transactions carried out by those business entities exceeded RUR 162 billion.

To assess the effectiveness of measures taken for mitigating ML risks in public sphere in 2019, database of Rosfinmonitoring was used for making relevant measurements which demonstrated the following positive dynamics:

- The amount of financial transactions carried out by contractors for transferring funds to shell companies decreased by more than two and a half times, and the number of such transactions declined almost threefold;

- The number and amount of financial transactions carried out by contractors, which are characterized by credit institutions as transactions intended for "cashing out" of public funds, decreased twofold;

- The number of financial transactions carried out by public contractors for transferring funds abroad declined by 25%, and the amount of such transactions decreased by 29%.

Despite the success achieved in mitigating risks in the budgetary sphere, there is an obvious need for further refinements in the current year.

The following is set as the priority for 2020:

- Determine at the legislative level the powers of Rosfinmonitoring to participate in treasury supervision, enforcement of the obligations and budget monitoring, *inter alia*, by sharing the necessary information with the Federal Treasury;

- Develop the structure of a unified classifier of risks in the framework of the applied approach to ensure traceability of achieving milestones and results of the national, federal and regional projects;

- Develop proposals for implementing the automated processes of preparing consolidated information on risks associated with national projects;

- Align the taken measures and achieved effects with the risks of accounting and reporting system;

- Develop additional measures for further improvement of analytical work.

RELEVANT ISSUES RELATED TO INFORMATION INTERACTION BETWEEN FEDERAL TREASURY AND FINANCIAL INTELLIGENCE UNIT OF THE RUSSIAN FEDERATION AS PART OF EXECUTION OF STATE BUDGET MONITORING

Monitoring of targeted and effective spending of public funds, preventing their embezzlement and misappropriation and ensuring compliance with the deadline for implementing public contracts are one of the key areas of collaboration between the territorial agencies of the Federal Treasury and Rosfinmonitoring

Sergei Bakhmatov,
Head of Risk Analysis and Assessment Division
Interregional Department of Rosfinmonitoring in the Northwestern Federal District

In order to implement such information interaction and assist the Federal Treasury in conducting budget monitoring of government contracts, the Agreement establishing the format and procedure of information sharing between the Federal Treasury and Rosfinmonitoring was signed in July 2017 pursuant to the *Regulation on Cooperation in the Framework of Budget Monitoring and Treasury Supervision by the Federal Treasury of Funds Allocated from the Federal Budget* (No.07-04-20/2 dated 14.11.2018).

Under this Agreement, the Federal Treasury provides Rosfinmonitoring with the information on government contracts funded from the federal budget, and Rosfinmonitoring, in its turn, informs the Federal Treasury about existence/absence of risks that may arise as a result of transactions with funds or other assets carried out in the course of implementation of the government contracts funded from the federal budget.

Since 2019, based on the information disseminated by Interregional Department of Rosfinmonitoring in the Northwestern Federal District in the framework of organized cooperation, the antimonopoly authorities conducted inspections in respect of the contractors suspected of being involved in shadowy schemes. These measures resulted in initiation of the administrative proceedings against a number of executive officers under Article 15.37, para.1 of the Code of Administrative Offences of the Russian Federation with subsequent imposition of administrative liability in form of fines in amount of RUR 45,000 and RUR 35,000, respectively.

Pursuant to the Decree of the President of the Russian Federation Vladimir Putin *on National Goals and Strategic Objectives of Development of the Russian Federation until 2024 (No.204 dated 07.05.2018)*, the national projects have been launched in 12 areas of strategic development, which are funded from the federal budget and shall provide for breakthrough research and technology advancement and social and economic development of Russia.

In this situation, one of the mechanisms that can be used for monitoring targeted and effective spending of public funds may involve mandatory treasury supervision of implementation of government contracts concluded as part of pursuing the objectives set in the National Projects Program.

Treasury supervision means the obligation of major recipients of public funds to open accounts in the Federal Treasury with subsequent presentation of documents confirming the use of such funds in accordance with the terms and purposes for which they are provided.

Pursuant to Federal Law No.459-FZ of 29.11.2018 *on Federal Budget for 2019 and for the Planning Period of 2020-2021* (as amended on 02.12.2019) advance payments made under government contracts in amount equal to and exceeding RUR 100 thousand are subject to mandatory treasury supervision.

Interregional Department of Rosfinmonitoring in the Northwestern Federal District regularly conducts analysis of all government contractors, information regarding whom has been received in the framework of organized interagency cooperation and, *inter alia*, is contained in notifications provided by the Federal Treasury Department in St. Petersburg, for identifying potential indications of breaches (risks) related to misappropriation or embezzlement of public funds.

In order to identify potential risks at the government contract execution stage, Interregional Department of Rosfinmonitoring in the Northwestern Federal District monitors such contracts in order to determine availability of information on possible failure to meet the deadlines for their implementation, identify senior managers and founders of organizations - government contractors involved in illegal activities, and collect other relevant and meaningful information for the contract monitoring purposes.

However, at present, there are no clearly defined and approved response measures to be taken by the relevant government authorities, *inter alia*, by the territorial agencies of the Federal Treasury, upon identification of potential risks related to conclusion of government contracts.

In view of this, the following provisions should be incorporated in the Budget Code of the Russian Federation:

- Create and maintain, in accordance with the order established by the Ministry of Finance of the Russian Federation in coordination with Rosfinmonitoring, a classifier of indicators of financial violations committed by entities that are subject to treasury supervision;

- Apply response measures, such as refusal to open Treasury account, prohibition from carrying out transactions on this account, etc., against entities that are subject to treasury supervision, *inter alia*, using information received with the help of interagency cooperation.

NATIONAL AML/CFT SYSTEM

ROSFINMONITORING SUMMARIZES 2019 RESULTS

A meeting of the Rosfinmonitoring Collegium entitled "Federal Financial Monitoring Service Performance in 2019 and Key Objectives for 2020" was held on 14 February 2020

The meeting was attended by Assistant to the President of the Russian Federation A. Seryshev; Deputy Chairman of the Government A. Overchuk; First Deputy Minister of Justice V. Pesenko; First Deputy Prosecutor General A. Buksman; Deputy Minister of Foreign Affairs O. Syromolotov; Deputy Chairman of the Bank of Russia D. Skobelkin; Head of the Federal Tax Service D. Egorov; Head of the Federal Treasury R. Artyukhin, Head of The Federal Service for Supervision of Communications, Information Technology and Mass Media A. Zharov; Acting Head of the Federal Customs Service R. Davydov; Head of the Assay Chamber D. Bril; representatives of the Presidential Executive Office, the Federal Security Service, the Ministry of Interior, the Investigative Committee, the Central Bank and other ministries and agencies.

Opening the Collegium meeting, Director of Rosfinmonitoring Yury Chikhanchin underscored that it is primarily necessary to review the challenges and threats faced by us at the international, national and ministerial level when assessing the results of the country's AML/CFT system performance in 2019.

Among the main international challenges identified by the Head of the Russian FIU was the evaluation of the Russian Federation by the Financial Action Task Force (FATF), which took place under conditions of severe political pressure. Following the results of the Mutual Evaluation Report, Russia ranked among the top five countries and its FIU among the top three for compliance with AML/CFT international requirements.

Yury Chikhanchin:

"We owe these results primarily to close cooperation between all AML/CFT system stakeholders and to the well-organized work of the Interagency Committee and the Interagency Working Group on Combating Illicit Financial Transactions, established by the President of the Russian Federation."

Another international threat stems from changes in strategies and tactics of terrorist organizations considering their new geographical location.

Yury Chikhanchin:

"The migration of terrorism-related individuals requires us to take steps to prevent the misuse of the Russian economic space for terrorist financing purposes."

At the national level the credit and financial sector, along with the ongoing migration of shadow and criminal proceeds from one financial sector to another, continue to pose a major problem. The main feature of rendering shadow services is their organized structure – "existence of management centre" and provision of infrastructure to be used by third parties.

In 2019, Rosfinmonitoring, working in collaboration with the Bank of Russia, the Federal Security Service, the Ministry of Interior, the Investigative Committee, the Federal Tax Service and the General Prosecutor's Office, managed to suppress activities of 25 shadowy platforms with the estimated turnover of RUR 38 billion.

Taken as a whole, the application by banks of protecting measures helped to prevent more than RUR 200 billion from entering the illicit market.

As part of the efforts to minimize the risks of abusing the country's judicial system for "cashing out" and transferring funds overseas for ML purposes, Rosfinmonitoring, acting as a third party, took part in almost 4000 proceedings. The total value of claims reviewed by Rosfinmonitoring exceeded RUR 150 billion. The number of rejected claims amounted to RUR 38 billion.

To prevent similar abuses, the Russia's Parliament has adopted amendments to the country's notary law developed by the Bank of Russia and the Supreme Court.

In general, the AML system demonstrates obvious reduction in the volume of suspicious transactions - on average by 20-30% annually, which is definitely a positive aspect.

In 2019, Rosfinmonitoring conducted approximately 4000 financial investigations, including involving more than 120 companies operating in the financial sector, of their possible participation in suspicious transactions. Relevant information was received from the Bank of Russia and law enforcement agencies.

As part of the efforts to combat high-level risks, Rosfinmonitoring in cooperation with the Federal Tax Service, the Bank of Russia and other AML/CFT system stakeholders brought the total number of shell companies to a historic minimum of 120,000 and reduced the total volume of transfers to their accounts by 1.3 times. It is recorded that the level of risks of using fictitious foreign economic activity for money laundering schemes has decreased.

To mitigate abuses in the precious metals and precious stones industry, Rosfinmonitoring works closely with the Assay Chamber. Meanwhile, collaboration with the country's four largest mobile network operators and

Roskomnadzor has led to a twofold reduction in the volume of suspicious transactions related to "cashing out" of funds involving transfers from shell companies to accounts of mobile phones subscribers, etc.

As part of the efforts to prevent and suppress tax crimes and criminal offences associated with budgetary funds, the focus was placed on public contracts, national projects and defence procurement.

To this end, Rosfinmonitoring in collaboration with the General Prosecutor's Office, the Federal Treasury, the Ministry of Interior, the Federal Tax Service and the Federal Antimonopoly Service is finalizing the development of a mechanism for identifying nominee legal entities and combating their activities in order to take preventive measures for ensuring the safety of public funds.

In cooperation with the Treasury, Rosfinmonitoring has already achieved positive outcomes in analysing usage of government subsidies allocated from the federal budget through Industry Development Fund. Rosfinmonitoring has identified financial transactions demonstrating misuse of public funds by machine-tool manufacture enterprises profiting over RUR 2.5 billion. The recovery of RUR 400 million to the federal budget has been initiated.

In the framework of mitigating corruption-related risks, Rosfinmonitoring conducted more than 4000 inspections and audits. Case materials of almost 190 financial investigations related to legalisation of criminal proceeds were sent to law enforcement agencies.

In order to comply with the anti-corruption legislation, Rosfinmonitoring conducted inspections of almost 90,000 individuals on the basis of 10 000 requests.

To protect the rights of individuals i.e. stakeholders of shared-equity construction projects, Rosfinmonitoring carried out over 320 inspections, including through the Interagency Working Groups under the Ministry of Construction and the General Prosecutor's Office. More than 1700 legal entities and 900 individuals became subject of inspections, over 500 case materials that are now being used in 400 criminal investigations were submitted. 60 proceedings were referred to court, resulting in 20

convictions. The total amount of reimbursement comprises RUR 750 million.

The decline, by the end of 2019, in the number of developer bankruptcies and unfinished construction projects shows a gradual decriminalization of the shared-equity construction industry.

Investigation files of Rosfinmonitoring were used to initiate 390 corruption-related criminal proceedings and 45 corruption-related ML criminal cases, resulting in the seizure of assets worth more than RUR 30 billion.

To minimize the TF risks, Rosfinmonitoring in collaboration with law enforcement agencies and the private sector carried out more than 10,000 financial investigations, submitting over 800 materials to law enforcement agencies. These materials were used to launch nearly 120 criminal investigations, including 65 TF investigations against 64 individuals initiated by the Federal Security Service, resulting in 20 convictions.

Rosfinmonitoring terminated the financial activities of over 4000 designated persons and entities freezing approximately RUR 38 million in their bank accounts.

In coordination with the Federal Security Service, Rosfinmonitoring was able to disrupt 5 major financing channels used by the Foreign Terrorist Organizations to transfer almost RUR 120 million for TF purposes.

Rosfinmonitoring jointly with the Ministry of Interior liquidated the ISIL's financing channel operating in Russia since 2014. It was used to transfer over RUR 500 million.

It is worth noting the results of the efforts of the Interagency Commission on Combating Money Laundering and Financing of Terrorism. In accordance with the Commission's decisions in 2019 the assets of 97 individuals and 1 entity totalling about RUR 5 million were frozen.

***

Below are the speeches of Rosfinmonitoring Collegium participants.

On the tasks for improving the national AML/CFT system to address the deficiencies identified in the FATF 4th round of mutual evaluations of the Russian Federation

A speech at the Rosfinmonitoring Collegium by German Neglyad, Head of Rosfinmonitoring's Legal Department

We were able to demonstrate to international assessors the effectiveness of our AML/CFT system. As a result, Russia was placed in the regular follow-up process, which was the best possible assessment outcome for us.

But it is not only international ratings that are important, but also of great importance is our AML/CFT system's ability to effectively cope with existing risks and threats and confront new challenges, as well as about our ability to adjust our efforts to meet the national goals and objectives.

The evaluation allowed not only assessors but also us to look at some things from a different perspective, to see certain aspects of AML/CFT technical compliance and effectiveness that need further improvement.

As for technical compliance, 5 out of the 40 Recommendations are rated PC, including 4 where the rating can be improved by adjusting the legal framework.

1. We need to ensure a prompt – within 24 hours – freezing of assets of UN designated persons. As a permanent member of the UN Security Council, it is our responsibility to set an example for other countries.

2. In the National Risk Assessment, the risk of misusing trusts for ML purposes was rated as high. We must regulate in the legislation of the Russian Federation the activities of Russian nationals managing foreign trusts, by including them in the list of reporting entities under the Federal Law No. 115-FZ. By the way, the Federal Tax Service faced the need to adopt similar amendments as part of its engagement with the OECD. The relevant draft law has already been prepared and is undergoing approval procedure by the Ministry of Economic Development and the Federal Tax Service.

3. As part of the implementation of FATF Recommendation 16 (Wire transfers), Rosfinmonitoring needs to cooperate with the Central Bank to determine the required framework of information which should accompany wire transfers, including the details about wire transfer beneficiary. This can be especially important for reducing the risks of drug-related money laundering and terrorist financing.

4. The legal status of virtual assets. Although this aspect was not formally scrutinized by the assessors because new amendments to the standards were out of the scope of assessment, it will be subject to monitoring during the assessment of progress. We need to ensure that the FATF requirements, along with the positions of the Central Bank, the Ministry of Finance, the Federal Security Service and the Ministry of Interior, are taken into consideration during the review of the relevant draft law by the State Duma.

With regard to effectiveness, there is also, in our opinion, some room for improvement.

As for the private sector preventive measures and respective supervision:

1. Assessors were concerned about the level of compliance by a number of private sector organizations with the responsibilities to organize internal control, customer due diligence and record-keeping.

In addition, certain number of financial institutions, unfortunately, continue to apply a rather formal approach to the identification of their customers' beneficial owner, by automatically assigning this status to the director or a person who, according to the Unified State Register of Legal Entities, predominantly owns the legal entity.

I believe that Rosfinmonitoring should collaborate with the Bank of Russia, the Federal Tax Service, Roskomnadzor and the Assay Chamber to improve its outreach to the private sector on aforementioned issues. It is also necessary to place additional emphasis on these aspects in the framework of supervisory activity by applying a risk-based approach.

2. Assessors highlighted significant volume of suspicious transaction reports sent to the FIU, which, according to the assessors, may complicate determination and selection of information requiring immediate attention. I think this is a fair point.

We should consider the issue of highlighting urgent and critically important reports, therefore amendments need to be proposed to the regulations of Central Bank and Rosfinmonitoring.

3. According to the assessors, separate targeted efforts should be dedicated to compliance of credit consumer cooperatives and the precious metals and stones sector, as well as casinos, real-estate agents and legal professionals, with mandatory requirements and their understanding of the ML/TF risks.

Indeed, the work to increase the level of law-abidance in these sectors should be continued.

Rosfinmonitoring in collaboration with the Bank of Russia, the Assay Chamber and the Federal Tax Service should develop a set of additional measures for these persons and entities, possibly, within the framework of federal and regional Compliance Councils.

With regards to improving the effectiveness of operational activities:

1. Assessors concluded that, due to the difficulties in proving guilt, prosecuted persons in Russia are ultimately accused of main offence which generated criminal proceeds or predicate or alternative offences, such as, for example, illegal banking activities, without having to face additional ML charges.

What could Rosfinmonitoring suggest here? It seems that analytical units should intensify their efforts to conduct proactive financial investigations and further improve their quality, including investigations of complex schemes involving professional launderers. At the same time, it is necessary to strengthen the coordination of intelligence sharing process with law enforcement agencies.

2. In the National Risk Assessment, Russia acknowledged the existence of high corruption-related ML risks. At the same time, assessors noted that the number of corruption-related ML criminal cases and convictions is hardly comparable to the total volume of relevant criminal proceeds.

The risk profile demonstrates that corrupt officials tend to generate their criminal assets in Russia but launder them abroad. Kuznetsov, a former Deputy Minister of Finance of the Moscow region is an example of such criminal activities.

I suppose that Rosfinmonitoring, in coordination with the General Prosecutor's Office, should enhance some aspects of its international efforts by focusing more on the tracing of corruption-related proceeds overseas.

In the area of CFT and application of targeted financial sanctions, Rosfinmonitoring should work more closely with the relevant departments of law enforcement agencies and the Ministry of Foreign

Affairs to include nationally designated terrorists in the international sanctions lists, as well as to intensify the use of the mechanisms for mutual bilateral freezing of terrorist assets both within the CIS and internationally.

In addition, it should be borne in mind that in June the FATF plans to incorporate into its standards the requirement for countries to assess the risks of evading CPF targeted financial sanctions. I think we should interact with the Ministry of Foreign Affairs, the Federal Security Service, the Federal Service for Technical and Export Control, the Bank of Russia and other supervisory authorities to begin preparations for such risk assessment right now.

During the preparation for evaluation, such interagency coordination authorities as the high-level IAC, creation of which was approved by the President of the Russian Federation, the IWG on Illicit Transactions under the Presidential Executive Office, Interagency AML/CFT/CPF Commission of Rosfinmonitoring, including the Advisory Board and Compliance Councils demonstrated their effectiveness.

The President of the Russian Federation supported proposal of Rosfinmonitoring to change the high-level IAC's mandate to address the shortcomings identified during mutual evaluation by the FATF. A corresponding draft regulation to be approved by the President has already been prepared.

Apart from that, Rosfinmonitoring has prepared a draft interagency roadmap to address the shortcomings identified during the mutual evaluation procedure. The document is aimed at a comprehensive review of all aspects of the Russian AML/CFT system included in the Mutual Evaluation Report. In December of the previous year, this approach was approved by the Interagency AML/CFT/CPF Commission. In the near future, we plan to finalize our work on this draft, taking into account proposals received from agencies, and submit it for approval by the renovated high-level IAC.

Systematic work is ahead, which, if properly organized, can bring significant benefits to society and the state.

Under current procedures, Russia is due to submit its follow-up report to the FATF in the summer of 2022 for consideration at the Plenary meeting which will take place in February 2023. Russia will need to report on implementation of the priority and recommended measures outlined in the MER, as well as on the technical compliance issues.

I express my gratitude to Rosfinmonitoring for joint fruitful cooperation

A speech at the Rosfinmonitoring Collegium by Anatoly Seryshev, Assistant to the President of the Russian Federation

The positive results announced today demonstrated that year 2019 produced good results in strengthening of the Russian AML/CFT system.

Here is a summary of 2019 achievements.

Firstly, according to outcomes of assessment by FATF, Russia is ranked among the top five countries for the effectiveness of AML/CFT system. The high ranking is particularly important for Russia in the context of the sanctions pressure, as it confirms the transparency and investment attractiveness of the country's financial market and our commitment to the fight against crime, corruption and terrorism.

Secondly, based on the performance of the Interagency Working Group on Combating Illicit Financial Transactions, the President of the Russian Federation approved a list of orders for creating a unified system of managing confiscated and seized property. We have been dealing with this issue for a long time, and now, I think, we are close to a systemic solution.

Thirdly, the methodological and analytical support provided to the Working Group by Rosfinmonitoring has allowed us to achieve significant results in improving the effectiveness of the regulatory framework in the area of bankruptcy of legal entities and cash turnover. Here we have also done a considerable amount of work and adopted mutually agreed decisions.

The activities of regional IWGs on combating illicit financial transactions, headed by the plenipotentiary representatives of the President of the Russian Federation in the federal districts, have been brought to a new level.

Separately, I would like to emphasize the enormous role in improving the quality of personnel training played by ITMCFM and the International Network AML/CFT Institute, which managed to utilise the best experience of educational practices. This is a very positive area of work, where, in essence, we effectively eliminate the existing barriers and contradictions arising between countries. Here you simply act as a reliable bridge and an assistant to the Russian state in terms of conducting negotiations and solving problems together.

I am convinced that we are becoming direct participants of major geopolitical changes, including the transformation of the economic models for the development of the countries - the

world's leading economies. This requires from all of us a high level of professionalism and a deep understanding of the processes occurring both within the country and abroad. The financial system is the blood system of the state, whose wellbeing is crucial for its viability and future development.

I'm grateful to the Rosfinmonitoring leadership and all its staff for their fruitful cooperation, a great contribution to the development of the country's trained staff, assistance to partner countries and promotion of our national interests on international platforms. I wish you all successful and fruitful work!

All necessary conditions are created for the achievement of ambitious goals

A speech at the Rosfinmonitoring Collegium by Alexey Overchuk, Deputy Chairman of the Government of the Russian Federation

On behalf of the Russian Government, I wish to convey my greetings and words of appreciation for the work done last year. The high ratings granted to Russia during the FATF mutual evaluation not only confirmed the maturity and effectiveness of the Russian AML/CFT system, but also highlighted our strengths in such areas as economic transparency, beneficial ownership and risk assessment. As a direct participant of this work, I can attest to the high quality of interagency cooperation organized by Rosfinmonitoring in the framework of preparation for the FATF mutual evaluation, during its work with the mission and directly at the FATF.

We worked as a team focused on achieving the result. It is an example that should be followed by all other federal executive authorities.

At the same time, the achieved results can be used for improving our regulatory framework. It gives us such an opportunity and we shouldn't miss it. These results can serve as a certain advantage in holding economic negotiations with our international partners and for promoting our ideas and achievements on the international stage.

Another big priority for 2020 is to give a new impetus to the integration processes within the EAEU. Today we are actively discussing with our EAEU partners the strategic areas of integration development until 2025. We are talking about the creation of a barrier-free environment, a common cultural space and free movement of goods, capital and labour. These are positive processes, but as professionals, you perfectly understand the ML/TF and drug trafficking risks related to these processes.

Therefore, integration is a good process, and Rosfinmonitoring plays a completely unique and special role here. In this region, Rosfinmonitoring

uses the format of the Eurasian Group on Combating Money Laundering and Financing of Terrorism (EAG) and the CIS Council of Heads of Financial Intelligence Units (CHFIU). Rosfinmonitoring definitely should find its place within the EAEU as a basic structure related to the economic security, which consolidates the efforts of the relevant agencies, CIS member states and international organizations.

I believe we should support an ongoing project of Rosfinmonitoring to establish an International ML/TF Risk Assessment Centre, along with its initiative to assess regional risks and develop a risk mitigation plan. We expect that the integration of these approaches will generate a real economic effect by eliminating criminal financial flows. Also, International Network AML/CFT Institute, developed by Rosfinmonitoring, has considerable growth potential. We should complete the institutionalization of this organization and, taking into account accumulated best practices, including experience in the training of highly-qualified financial security experts from among EAEU nationals, this Institute can become a CIS backbone training centre specializing in a wide range of economic issues. In general, the technical assistance programmes for the partner countries, in the implementation of which Rosfinmonitoring also has extensive experience, i.e. promotion of Russian best practices, some of which are unique, are one of the main areas of economic integration. Here we need to use existing experience of Rosfinmonitoring to achieve maximum results.

The development of the BRICS format, which is another important area of our international cooperation, has become one of the priorities of Russian presidency for 2020. Here Rosfinmonitoring has initiated the creation of an international legal mechanism for the recovery of criminal proceeds which were moved out of the country. I hope this initiative will continue its development in the UN, in coordination with the Ministry of Foreign Affairs and law enforcement agencies, and will be successful. This should become our priority.

Meanwhile, our core objective, set by the President of the Russian Federation, is to achieve the country's development goals through the implementation of national projects. This is the top priority of the Russian Government. One of the main conditions of its attainment is our ability to monitor their implementation and ensure the proper expenditure of budget funds allocated for them. Here the FIU plays a key role. I think Rosfinmonitoring will play an important role in monitoring the execution of national projects, as pointed out by M. Mishustin [Chairman of the Government of the Russian Federation] recently.

It is common knowledge that Rosfinmonitoring has already developed successful result-oriented mechanisms for monitoring and assessing the risks of misusing budgetary funds. These efforts require further consolidation, improvements and development, and I know that you give priority to this, and want you to continue to do so.

Year 2020 began with the setting of ambitious goals. All necessary prerequisites and conditions for their achievement have been created. I wish you success in your work, and I am confident that you will continue to demonstrate a high level of professionalism and creative approach which is specific for Rosfinmonitoring.

Among our priorities are legislation development aimed at increasing transparency

A speech at the Rosfinmonitoring Collegium by Daniil Egorov, Head of the Federal Tax Service of the Russian Federation

I would like to highlight several points of our work and first of all start from the international aspect.

In addition to what Alexey Overchuk [Deputy Chairman of the Government of the Russian Federation] said about the high-quality work that was demonstrated to protect the interests of Russia during the FATF mutual evaluation, I would say that it is the best practice for any agency preparing for an international assessment. I think we all benefit from it because we witnessed very high-quality preparation for this event. What is more, we ourselves are due to undergo an assessment by the International transparency forum this year.

As part of preparation for this event, we need, among other things, to introduce legislative amendments to improve the level of transparency.

There are situations which demonstrate substantial level of risks. By their nature, these risks fall into several categories.

Firstly, it concerns access to information on beneficial owners. Tax authorities currently don't have direct access to this information, which obviously affects our ratings in the framework of international transparency.

Secondly, the definition of a beneficial owner given by the Federal Law No. 115-FZ is too concise. It should be enhanced to facilitate the identification process focusing on the behaviour of financial market participants. And here we have referred to the EU practices and directives related to the identification of beneficial owners. I believe that we can use some aspects of this EU experience.

Thirdly, we come to accounting systems. By now, we are to understand that the beneficial owner is not only an element covered by 115-FZ, it is a subject that affects a large number of legal relations. Therefore, given the availability of the registers of legal entities and individual entrepreneurs, it is only a matter of time before we face the need to establish a register with systemic clear access to this information.

The next element is the system of government contracts both in the framework of defence procurement and national projects. We understand that we also need to work on the systematization of both subjects and objects. Today, we don't have a unified register that we can use to work element-by-element.

And finally, in 2019, based on the information received from Rosfinmonitoring, we charged additional tax amounting to over RUR 14 billion.

That obviously includes unjustified tax benefits and the value added tax. If we convert this into contracts amount, we will get a sum of more than RUR 230 billion, allocation of which raises a big question. With high probability, a large proportion of this amount, which is now subject to additional tax liabilities, is made up of bribes and overstated contract value.

We must continue to apply a systematic approach to our work here.

I see little point in mentioning those RUR 14 billion as an achievement, since, ideally, this amount should not exist at all. If we can work harder to prevent such cases, then the value of our work will increase significantly.

Cooperation between General Prosecutor's Office and Rosfinmonitoring covers all focus areas

A speech at the Rosfinmonitoring Collegium by Alexander Buksman, First Deputy General Prosecutor of the Russian Federation

On behalf of General Prosecutor of the Russian Federation, Igor Krasnov, who has been interacting with Rosfinmonitoring for many years as part of his previous job, I would like to convey to you his congratulations, best wishes and gratitude.

I cannot imagine an area of supervisory activities where we do not collaborate with Rosfinmonitoring. At the same time, I would like to focus on the topic related to national projects. We should never come back to – but instead learn from – the negative experience associated with the construction of the Vostochny spaceport: over a hundred convictions, dozens of persons under investigation and on trial, billions of roubles stolen, little recovered and, most importantly, the construction object is yet to be completed. For this reason, we need to do our best to ensure that the enormous amounts of funds allocated for the implementation of national projects are only used for intended purposes.

We should move towards online interaction forms in order to understand at initial stages where the funding goes, if it is used as intended. In this regard, we rely on your prompt reporting.

The General Prosecutor's Office and Rosfinmonitoring have also achieved good results in monitoring the banking sector.

I wish you all success in your future work and hope for even closer cooperation in all fields of activity.

Our work allowed us to prepare Russia for a successful evaluation by the FATF

A speech at the Rosfinmonitoring Collegium by Valery Pesenko, First Deputy Minister of Justice of the Russian Federation

As part of the implementation of powers vested by the State, the Ministry of Justice maintains ongoing interagency cooperation with the Federal Financial Monitoring Service in the number of important areas of activities.

Thus, our agencies worked together to prepare and undergo the FATF 4th round of mutual evaluations. One of the positive aspects of the FATF recent assessment was that it provided the Ministry of Justice with the opportunity to conduct an internal audit of existing processes: the purpose, assessments and their contribution to the national AML/CFT system. Among significant areas of work, which became subject to analysis, were non-profit organizations, representatives of the designated non-financial businesses and professions, including lawyers and notaries, and international activity.

This work allowed us to identify problems and assess terrorist financing risks faced by Russia for the subsequent adoption of measures necessary to eliminate and prevent them and to successfully undergo the FATF fourth round of mutual evaluations. Considering the conducted national and sectoral risk assessments, interagency cooperation is implemented not only in enforcement area but also in the framework of legal regulation. The Ministry of Justice is one of the competent bodies responsible for implementation of rights and the fulfilment of obligations arising from multilateral and bilateral international treaties of the Russian Federation addressing such issues as legal assistance and legal relations, including criminal case matters.

An internal review undertaken by the Ministry of Justice in this area revealed the need for an additional collection of statistical information in the framework of the provision of international legal assistance in criminal matters to address requests for the confiscation of criminal proceeds.

Moving to another area of our cooperation, it is worth noting that the work carried out by NPOs is a source of civil initiatives capable of reflecting social interests and, to some extent, ensuring social stability and civil peace in the State. At the same time, the existing threats and their possible consequences as well as attempts to impose extremist and terrorist ideology make it necessary to pay special attention to the prevention and detection of such manifestations in the activities of NPO sector. For information, there are currently 213,000 NPOs operating in Russia, with 13,000 new ones being registered every year.

Rosfinmonitoring and Ministry of Foreign Affairs have established relations of a true partnership

A speech at the Rosfinmonitoring Collegium by Oleg Syromolotov, Deputy Minister of Foreign Affairs of the Russian Federation

I would like to join the congratulations expressed by the team of Rosfinmonitoring and the rest of us on the completion of the FATF 4th round of mutual evaluations.

In the face of certain countries' attempts to restrain Russia, the conclusions made by the FATF are extremely important for strengthening Russia's positions on the international arena and for improving its business reputation and investment attractiveness. These results will be referred to by all international organizations, including the UN, the International Monetary Fund, the World Bank, OECD, the Council of Europe, etc. The achieved high level must be maintained. It is evident that Rosfinmonitoring is working on a plan to address the identified concerns.

Considering non-diminishing terrorist threat, this work is particularly important because international terrorist organizations are actively looking for new channels and new funding sources.

Terrorists more often use technologies which complicate the identification of money remitters and recipients. Two cases of terrorist groups demanding ransom for hostages to be paid in bitcoins have already been recorded in Cameroon and Chad. In other words, a precedent has already been set.

AML/CFT issue requires a substantive discussion, primarily within the framework of Interagency commissions and Councils established by Rosfinmonitoring. We believe they are very effective, and experts of Ministry of Foreign Affairs are ready to take part in their work.

As seen from the foreign policy perspective, we should do more to share the acquired experience with our key partners, primarily within the CIS.

We highly appreciate efforts of Rosfinmonitoring to provide technical assistance to our foreign partners. In this regard, I would particularly like to highlight our project cooperation with UNODC in the training of specialists for the countries of Central Asia and Southeastern Europe. A huge contribution to these efforts is made by the International Training and Methodology Centre for Financial Monitoring, as confirmed, among others, by our international partners.

As you know, last September the Ministry of Foreign Affairs hosted the second international conference "Combating Illegal Arms Trafficking in the Context of the Fight against International Terrorism." The discussion revealed various ways of obtaining and using weapons and military equipment by terrorist groups. It is clear that they receive it using different sources of funding. It is important to continue to draw the attention of the international community to the fact that any financial and material support of terrorism should not be tolerated. The Syrian and Iraqi armies are not the weakest in the world. ISIL had been quite successful at fighting against them before Russia decided to address this process.

In other words, the quantities of arms it receives, including high-tech, which cannot be hidden, is sufficient enough to fight whole armies.

We highly appreciate the work made by Rosfinmonitoring on strengthening the legal framework of international cooperation, taken forward last year with the intergovernmental agreement with Mongolia on cooperation in the fight against terrorism. Last year Russia became a participant of the Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism. In order to implement the provisions of this Convention and submit the timely reporting, Rosfinmonitoring, the General Prosecutor's Office and the Ministry of

Justice will have to work hard jointly with the Ministry of Foreign Affairs which plays a coordinating role.

With regard to future prospects, following the transition of the BRICS Presidency to Russia in January 2020, the institutionalization of the BRICS AML/CFT Council will become one of the priorities. Informal meetings in this format on the margins of the FATF and EAG Plenaries have long proven their effectiveness. But now the time has come to use this experience within the BRICS. I do not want to exaggerate, but I must say that in the course of their cooperation Rosfinmonitoring and the Ministry of Foreign Affairs have established partnership relations, which, we are convinced, will continue in the future.

We are open for further dialogue and cooperation

A speech at the Rosfinmonitoring Collegium by Alexander Zharov, Head of the Federal Service for Supervision of Communications, Information Technology and Mass Media (Roskomnadzor)

Our cooperation is practice-oriented. Roskomnadzor, which has been part of the AML/CFT system since 2002, works with 2 federal postal service operators, 84 mobile network operators and 10 major telecommunications companies. Rosfinmonitoring's cooperation with the Russian Academy of Sciences will soon pave the way for the integration of artificial intelligence and neural networks into the monitoring systems.

We also work closely with the Russian Academy of Science Federal Research Centre exploring the use of neural networks for monitoring purposes. We are ready to combine our efforts in this area, since we have common point for its application.

The use of a risk-based approach to supervision in the communications industry has been one of the latest trends here, allowing us to reduce the number of scheduled inspections in the supervised sectors from 113 in 2018 to 102 in 2019. In the future, we also plan to place a greater emphasis on organization of remote methods of control and monitoring and on adoption of preventive measures aimed at compliance with AML/CFT requirements. It is obvious to us that over the past 17 years, preventive work and ongoing outreach to telecommunications companies have yielded good results. The number of violations identified in this area has declined approximately twofold. Meanwhile, our future plans include the following:

1. Updating the communications service providers on the existing and emerging ML/TF risks. On the main page of the Roskomnadzor website there are special sections used by communications service providers. It certainly gives its effect.

2. Making full use of a new form of information interaction - Roskomnadzor's Personal account on the Rosfinmonitoring website.

3. Further upgrading of the Personal account on the Roskomnadzor website.

4. Focusing on preventive measures.

5. Further improvement of Roskomnadzor's regulations in compliance with international requirements and standards.

Roskomnadzor is actively involved in the EAG's AML/CFT international efforts and all these have become a good methodological basis in the framework of preparations for the key event i.e. FATF 4th round of mutual evaluations.

I would like to congratulate everyone on the outstanding result: the 5th place in the world is a big achievement! In the future we also plan to participate in these processes together with you, and are open for further dialogue and cooperation.

We plan to improve the Assay Chamber's management structure

A speech at the Rosfinmonitoring Collegium by Denis Bril, Head of the Russian State Assay Chamber

In 2019, the Assay Chamber conducted 861 inspections to check compliance with AML/CFT requirements.

Information provided by Rosfinmonitoring became the reason for conducting 488 inspections (57% of the total). Information uploaded by State Inspection from supervisor's Personal account resulted in carrying out 182 inspections (21% of the total). Thus, the total number of inspections, conducted on the basis of the information provided by Rosfinmonitoring and analysis of data from supervisor's Personal account, comprised 670 (or 78% of the total).

These figures clearly demonstrate the level of our cooperation. The aforementioned inspections resulted in 291 warnings, 127 administrative

penalties, 9 administrative suspensions of operation and 292 remedial orders. Although these results are still quite modest, we expect to see a qualitative increase in the effectiveness of our performance this year.

At the end of last October, the President of the Russian Federation signed a decree establishing the Federal Assay Chamber as a Federal Service. The new powers granted to us by this decree must be used as efficiently as possible to achieve our goals. Today we have a clear understanding of the Assay Chamber's future development prospects, we also learn from your experience and we hope to be of greater use as a partner in this area of activity.

With regard to the focus areas of development, we plan to improve our management system and primarily develop and implement a strategic planning system in the Assay Chamber, including performance assessment and motivation mechanisms to cover not only the agency as a whole, but also its structural divisions and individual employees. Ever since its establishment, the Federal Assay Chamber has been working – cooperating with Rosstat and Rosaccreditation – on the implementation of GOST ISO-900 standards.

Regarding the development of information technologies, we are focusing not only on performance improvements and, definitely, interagency cooperation, but also on effective preventive measures.

USING FEEDBACK AS MECHANISM TO IMPROVE THE QUALITY OF SUSPICIOUS TRANSACTION REPORTING

The issue related to improving efficiency of providing information by reporting entities has long become one of the main problems of organizing supervisory activities, despite the fact that the FIU is the main consumer of this information

Alexander Kuryanov,

Deputy Head of Rosfinmonitoring's Supervisory Activities Department

According to the mutual evaluation results, vulnerabilities and shortcomings in suspicious transaction reporting tend to affect the country's ratings for several Immediate Outcomes (IOs). This is true not only for IO 4, where reporting is set out as a separate criterion, but also for IO 6, which outlines the effectiveness of FIU efforts, and in some cases even IO 3.

When analysing the effectiveness of the national AML/CFT regime, international experts tend to focus on the macro statistics related to the dynamics of suspicious transaction reports (STRs). However, following the previous experience, the assessed country should provide STRs statistics broken down not only by year and type of reporting entities, but also by the criteria of suspicion, according to which STRs were submitted. It is also advisable to provide the STRs structure based on the level of transaction risk. And finally, the assessment team receives STRs statistics breakdown related to ML, TF and, preferably, attempted transactions.

As for relative indicators, it is recommended to use financial investigation index as this indicator shows the level of STRs transformation into specific financial investigations.

At the same time, despite its significance, countries are not advised to limit their actions to the aforementioned focus area, since STRs may also be used for tactical and strategic analysis, in supervisory activities and during assessment of reporting entities' compliance risks, etc.

Meanwhile, another key aspect of a successful suspicious transaction reporting strategy is the outcomes of interviews with the private sector. When evaluating financial institutions, assessors focus on the procedure and STRs formation processes from the moment alerts are triggered until the completion of the reporting form. Assessors pay attention to the ratio of volumes of daily generated STRs with the number of compliance employees tasked with analysing and filtering out the data generated in response to red flags.

Existing best practices reviews demonstrate that such level can reach 90%, i.e., out of 100 transactions selected based on the results of alerts, only 10 are classified by authorized employees of financial institutions as suspicious. These 10 reports have been formed through an in-depth analysis of the client's economic activity, his/her sources of funds or wealth; correlation of this data with beneficial ownership information; and analysis of contextual data.

The level and volume of analytical processing of transactions are also demonstrated by the decision-making process related to the submission/non-submission of STRs, as well as by their information content. All countries filing STRs have the opportunity of describing in details the circumstances which resulted in classifying the transaction as suspicious in the designated field within the STRs form. It is considered a good practice to include in this field not only information on a single transaction, but also schemes with a list of names and description of participants. This approach, however, is typical for reporting practices applied in the Anglo-Saxon system. In addition to alerts, it is also important for STR regime to describe any additional circumstances that led to the classification of the transaction as suspicious.

The share of STRs not generated on the basis of established indicators and red flags is used as evidence of analytics when processing STRs and the effectiveness of detecting new risks. In Russia, reporting entities use the so-called "other codes" to submit STRs if the transaction doesn't meet the existing indicators, i.e., when they independently identify suspicious transactions based on a set of objective and subjective factors.

The analysis of STRs filed by non-financial businesses and professions is slightly different. Here, in addition to the total number of STRs, the assessment criteria also include reporting statistics and, importantly, the number and share of reporting entities. Many sectors are characterized by high concentration levels: when 90% of reports are generated by several reporting entities. This is perceived negatively by assessors, who often draw conclusions not only about ineffective STRs regime, but also about reporting entities' poor understanding of the risks, which affects the compliance with IO 1 and IO 3.

In this regard, assessors pay extra attention to the report structure in terms of reporting sectors, believing – quite rightly – that it should closely correlate with the risk level of a specific sector i.e., sectors with high and substantial level of risk should submit more reports than those with low or moderate level of risk. This aspect needs to be taken into account, and it is recommended to conduct more intensive preventive and outreach activities in these vulnerable sectors in order to raise reporting entities' awareness of the existing legal requirements and risks.

This systemic and targeted approach to the sector – when the supervisor issues STR guidelines and recommendations accompanied by simple, specific case studies, when easy to perceive typologies are communicated to reporting entities, and when supervisor explains the importance of STR submission and how they are subsequently used –definitely helps to achieve the best results.

Meanwhile, when assessing compliance with STR requirements by DNFBPs, assessors, taking into account the sector specifics, including occasional types of services, focus not so much on objective factors but on subjective aspects which are involved in classifying transactions as suspicious, such as the client's suspicious behaviour, excessive nervousness and haste, concern about ongoing CDD procedures, etc. Casinos, for example, may use corporate analytical monitoring tools or video investigations to identify unusual customer behaviour.

It is particularly important to develop guidelines on specific activities with a description of specific cases. When countries demonstrate effectiveness of such work i.e. publication of guidelines and recommendations leads to the increase in the volume of STRs, assessors consider it as good practice.

Another area of the assessors' focus is the timeliness and urgency of suspicious transaction reporting. In this regard, it is important for the FIU and supervisors to place emphasis on this aspect and take relevant measures in collaboration with reporting entities.

In the Anglo-Saxon countries, it is quite common to submit reports labelled as high risk, i.e., when there is a strong indication that the transaction is linked to ML/TF. Typically, such a report is sent within 24 hours from the moment of the transaction. The rationale behind this approach is as follows: when a financial institution has a clear indicator that the transaction is related to ML, it, instead of undertaking enhanced CDD, promptly files an STR marked as high risk to the law enforcement agencies for the necessary follow-up.

Predictably, much of the assessors' attention is devoted to TF related transactions. The volume of TF STRs definitely needs to be consistent with the country's risk profile, but a low volume of TF STRs is often deemed by assessors as the reporting entity's poor awareness of these risks.

Feedback, provided by government agencies in response to submitted STRs, is a key element of an effective suspicious transaction reporting system. The best feedback practices were summarized in the 2006 special guidance published on the OECD website. Not only reporting entities but also associations, law enforcement agencies, financial regulators and other government bodies benefit from the provision of feedback. The guidance underlines the need to avoid the risk of disclosing information about ongoing law enforcement investigations when providing feedback.

The guidance focuses on the fact that some countries have strict laws prohibiting FIUs from disclosing certain types of information. However, the competent authorities should try to develop feedback mechanisms and procedures that are consistent with their laws and administrative systems; take into account such practical and legal restrictions; and strive to provide an appropriate level of feedback. In other words, limitations should not be used as an excuse to avoid giving feedback, although they may provide strong reasons for the flexible use of these guidelines in order to ensure an adequate level of feedback by reporting institutions.

There are several reasons why the provision of feedback is important. The main reason is that feedback is one of the ways in which the government and law enforcement agencies can strengthen their partnership with the financial sector. Furthermore, feedback provides the information which demonstrates to the financial sector that the resources and efforts invested by it in suspicious transaction reporting are not wasted and produce tangible results.

Empirical data show that robust feedback and collaboration with reporting entities, especially the non-banking sectors, always result in a sharp increase in the number of STRs.

The guidance highlights the most common forms of feedback, including the ML/TF typological research carried out by national agencies, which, according to the guidance, should be made available for the private sector along with similar FATF documents, as well as the sanitized ML/TF case studies, which are prepared in cooperation with Interpol.

Actually, case studies used by countries that apply this form of feedback are usually criminal cases and criminal proceedings which have been completed either because of the completion of criminal proceedings or because the decision to report a suspicious transaction or suspicious client's activity was not justified. The inclusion of such cases is also considered useful.

Each sanitized case study should include:

- a description of the facts;

- a summary of the investigation outcomes;

- where necessary, a description of the FIU's requests; and

- a description of the aspects, techniques and approaches that characterize an effective reporting regime, i.e., the lessons that should be learned from a given case. This can be useful not only for financial institutions and their employees but also for law enforcement agencies.

The basic information used for general feedback may include statistics regarding the number of STRs and financial investigations initiated following STRs review.

Statistics, which are the most common form of feedback, tend to be included in annual reports or regular newsletters, such as those published by the FIU.

To ensure the effective use of human resources, statistics should ideally be published annually to provide an adequate feedback in most countries.

It is important for the management not to be limited to these types of feedback and instead allow for other forms and themes of private sector interaction on suspicious transaction reporting.

Among the most common forms of feedback are annual reports and regular newsletters, or circulars. As noted above, annual reports may contain useful statistics and descriptions of money laundering trends. A short (i.e., four-page) newsletter or circular published on a regular basis two or four times a year helps maintain an ongoing contact with reporting entities. It may contain sanitized case studies, new laws and information on the current money laundering schemes.

Some FIUs provide feedback during in-personal meetings with representatives of financial institutions.

Many countries and financial institutions or their associations have published training video courses, as this communication format creates opportunities for direct feedback to the AML/CFT units and front office staff.

Speaking about specific countries, we can cite the UK approach as an example. The official FIU website of this country contains a large volume of information devoted specifically to reporting by obliged entities. Moreover, papers are targeted at different audience – depending on the level of their immersion in the subject.

The website also provides explanations of even such basic points as where reports are sent and what happens to them afterwards. As is known, the UK uses a multipoint reporting system whereby the main body of reports is accessible directly to law enforcement agencies, while the highly sensitive information is either retained by the FIU or sent exclusively to specialized law enforcement units.

Annual reports published by the FIU tend to contain a statement by its director about the importance of effective reporting, information from guidelines, statistics and examples of using information. Sanitized case studies are published quarterly in special bulletins, which are also available on the website. Visitors can also find detailed examples of reporting and completing STR form.

I would like to say a few words about our system. Last year we began to provide analytical feedback to the management of major banks on the use of their information, including on existing problems and possible solutions.

Rosfinmonitoring considers the Compliance Council, established at the end of 2015, as the main feedback mechanism. Currently, the Compliance Council serves as an important channel for sharing information on emerging risks. At its meetings, representatives of Rosfinmonitoring disclose STR statistics from different analytical perspectives and provide feedback on the timeliness of reporting practices, i.e., the average number of days it takes for financial institutions to classify a transaction as suspicious. The Compliance

Council has recently become involved in the work to compile best prevention practices for inclusion in case study albums.

To facilitate feedback provision, Rosfinmonitoring uses both IT technology and the main RegTech tool – the Personal Account on the website of Rosfinmonitoring – where brief quarterly STR analytical reviews for each sector are prepared and published.

Rosfinmonitoring is currently engaged in the pilot testing of another IT project related to the communication of the information flow quality index to financial institutions through the Personal Account. The new approach involves the use of certain algorithms to rate the financial institution's compliance with the key criteria related to reporting effectiveness (timeliness, focus on risks, and the level of cooperation with the FIU) and on this basis performing integral assessment.

INTERNATIONAL BLOCK

FATF PLENARY FOCUSED ON EFFECTIVENESS

Interagency delegation headed by Rosfinmonitoring (A. Petrenko) and comprised of the representatives of Ministry of Foreign Affairs, Federal Security Service of the Russian Federation, Ministry Of Interior, Investigative Committee and Bank of Russia took part in the FATF Plenary meeting held in France 16–22 February 2020

The OECD restrictions on visits of its headquarters by China representatives, imposed in response to the spread of coronavirus, did not allow them to attend this event. The only exception was Xiangmin Liu, the FATF President.

The inability of the delegates placed under quarantine to be physically present at the meeting was compensated by the organization of videoconferencing.

As a response to the threat posed by the deterioration of the situation related to the COVID-19, it is very likely that the upcoming FATF/EAG joint Plenary Meeting, scheduled to take place in Suzhou this June, will be moved to Paris. In this case, the FATF Secretariat will take steps to organize this event at the OECD headquarters.

The Plenary elected Marcus Pleyer (Germany), the representative of Ministry of Finance, as the next FATF President. His term will begin on 1 July 2020, and he will be the first FATF President with a two-year term. Marcus Pleyer currently holds the position of FATF Vice-President.

For the first time in the FATF history, a meeting of the key Policy Development Group (PDG) was co-chaired by a Russian representative, Yu. Lafitskaya (Rosfinmonitoring), who won the contest for filling a vacant position within the PDG leadership held in November-December 2019.

The central topic of the Plenary meeting was the strategic review of the FATF key procedures and focus areas to improve their effectiveness. The idea of introducing thematic and risk-based assessments instead of traditional ones was actively promoted by a number of delegations. Meanwhile, Russia advocated the need to retain the current working principles and the tried-and-tested system based on impartiality and integrity, which provides an opportunity of assessing all closely integrated elements of the national AML/CFT framework.

One of the most urgent issues on the agenda concerned changes in the FATF standards in terms of assessment of proliferation financing risks. Following the discussion, it was decided to finalize the list of amendments in the summer of 2020.

The FATF is strengthening its efforts to analyse the requirements related to the increased transparency for legal entities, in order to finally understand whether there is any need to change the existing standard (FATF Recommendation 24). The organization has approved the mandate of the project group to

be co-chaired by Russia (FTS) and the UK, which demonstrated high level of effectiveness in this area.

Following the review of the Republic of Korea and UAE's reports on the effectiveness of their AML/CFT systems, both countries were placed under increased monitoring (annual reporting), with the UAE to be in the pool of jurisdictions-candidates for the inclusion in the FATF 'grey list'. These decisions still require approval by the FATF Global Network, after which the reports will be published.

Given Iran's failure to ratify the Palermo Convention and the International Convention for the Suppression of the Financing of Terrorism, the Plenary decided to lift the moratorium on counter-measures against Iran.

Such countries as Yemen, Mongolia, Syria, Pakistan and other countries are already included in the FATF 'grey list'. Albania, Nicaragua, Mauritius and Myanmar have also been placed on this list.

After the recent publications in the media, in which several jurisdictions were mistakenly referred to as members of the FATF 'black list', steps have been taken to significantly simplify the introductory part of the FATF public statement, which will now be called "High-Risk Jurisdictions subject to a Call for Action."

On the margins of the Plenary meeting, the Russian delegation held bilateral negotiations with the French financial intelligence unit (TRACFIN), which is celebrating its 30th anniversary this year.

In addition, employees of the International Training and Methodology Centre for Financial Monitoring (Evgeny Legostaev, Anna Bulaeva and Konstantin Sorokin) received letters of appreciation on behalf of Chairman of Kazakhstan's Financial Monitoring Committee of the Ministry of Finance for providing assistance in creating an e-learning training course for Kazakhstan's supervisors and financial monitoring stakeholders entitled "Role of Organizations in the Fight against Money Laundering and Terrorist Financing."

TRAINING OF LAW ENFORCEMENT EXPERTS IS A TOP PRIORITY

The EAG assessors training workshop "Assessment of effectiveness, experiences and best practices in ML investigation in Eurasian region" was held on 11–15 November 2019 in Tashkent (the Republic of Uzbekistan). The workshop was jointly organised by EAG, OSCE, UNODC and ITMCFM and was attended by over 40 representatives from EAG member states and key AML/CFT international organizationsmember

Inessa Lisina,
Deputy Editor-in-Chief

Ongoing personnel training and strengthening of the national anti-money laundering systems of member states are EAG's priority activities. During the 2nd round of mutual evaluation EAG attention is devoted to the efficiency and effectiveness of AML/CFT efforts, hence EAG is focused on assessors training, particularly of the law enforcement specialists. That`s why target audience of the workshop primarily consisted of practice-oriented prosecutors, specialists from investigation public authorities and FIU staff from EAG member states.

Participants were greeted by Dilshod Rakhimov, the head of the Department for Combating Economic Crimes under the General Prosecutor's Office of the Republic of Uzbekistan. The country's leadership pays special attention to AML/CFT issues, which pose not only national but also global threat to stability and security. Investigation of ML offences is a complicated and time-consuming process requiring coordination at the national and international levels. The complexity of this task explains the composition of the training participants and invited trainers.

In his welcoming remarks to the participants, Sergey Teterukov, EAG Executive Secretary, mentioned that the wide diversity of the workshop participants allows representatives of various AML/CFT agencies to get more information about activities of each other. The workshop, according to him, has two main objectives. First, it helps EAG member states to build effective AML/CFT systems that meet the requirements of international standards, and second, it gives knowledge for successful preparation for mutual evaluation.

Both objectives are aimed at achieving EAG main goal: to train a pool of assessors ready to take part in the next round of mutual evaluation. In this regard, the workshop agenda included three main sections which covered all aspects of experts training. The first section consisted of EAG member states practitioners` presentations, who shared experiences and best practices in confiscating criminal assets, conducting investigations, ML typologies, international cooperation, and parallel financial investigations. Specific examples and facts based on the experience of partner states assisted participants in better understanding of ML/TF risks facing the region, as well as in identifying common challenges and priorities.

These presentations were supplemented by contributions from international experts who took part in on-site visits in the framework of the previous round of mutual evaluations. Meanwhile, presentations on FATF and FSRB requirements were made by the EAG Secretariat representatives.

This knowledge was used by the participants in a series of practical tasks, including exercising in taking interviews with representatives of the assessed country (on-site visit), and preparation and presentation of a mutual evaluation report.

The format of this event allowed participants to gain comprehensive knowledge about IO 7 "Money laundering offences and activities are investigated and offenders are prosecuted and subject to effective, proportionate and dissuasive sanctions," IO 8 "Proceeds and instrumentalities of crime are confiscated" and IO 2 "International cooperation delivers appropriate information, financial intelligence, and evidence, and facilitates action against criminals and their assets" assessment and rating. In the future, they can use this information not only to prepare their countries for mutual evaluation procedures, but also to participate in on-site visits as assessors.

TRAINING ON FATF CPF STANDARDS

The joint EAG/FATF TREIN/ITMCFM counter proliferation financing training was held on 9-12 December in Moscow. The workshop was attended by employees of national anti-money laundering systems from EAG member states

Inessa Lisina,
Deputy Editor-in-Chief

In her opening remarks, Deputy Director of Rosfinmonitoring Galina Bobrysheva highlighted the importance and relevance of the training course programme for the preparation and conduct of the EAG 2nd round of mutual evaluations. Training topics are of a great practical importance for all EAG member states, allowing the course participants to gain new knowledge and assistance for better understanding of the FATF CPF requirements for assessed countries.

At the same time, national AML/CFT systems` participants from EAG member states should share the information received during the training with representatives of the private sector, particularly as it pertains to the actions to be taken to facilitate the implementation of targeted financial sanctions.

Guillermo Rodriguez, Acting Director of FATF TREIN, thanked the EAG Secretariat and the ITMCFM staff for work in preparing the training. In his speech, ITMCFM General Director Evgeny Legostaev welcomed his counterparts from the FATF Training Centre as well as all other training participants.

EAG Executive Secretary Sergey Teterukov also thanked the Russian Federation and the ITMCFM management team for organizing the training and for assisting representatives of EAG member states in their participation in it. In his opinion, this workshop is particularly important for representatives of four EAG member states that are preparing to undergo mutual evaluation procedures, as it will allow them to use the acquired knowledge for better preparation for the upcoming on-site visits.

The structure of the training was designed to achieve the stated goals. The theoretical part of the training included a review of the requirements of Recommendation 7 "Targeted financial sanctions related to proliferation" and parts of Recommendation 2 "National cooperation and coordination" related to proliferation financing.

The implementation of these and related Recommendations influences countries' effectiveness rating in line of Immediate Outcome 11 (IO11) – "persons and entities involved in the proliferation of weapons of mass destruction are prevented from raising, moving and using funds, consistent with the relevant UNSCRs".

Compliance with other proliferation financing requirements is also assessed in the framework of IO 1 – money laundering and terrorist financing risks are understood and, where appropriate, actions are coordinated domestically to combat money laundering and the financing of terrorism and proliferation.

More information on proliferation financing can be found in the FATF Guidance on Counter Proliferation Financing "The Implementation of Financial Provisions of United Nations Security Council Resolutions to Counter the Proliferation of Weapons of Mass Destruction" of February 2018. The Russian translation of this document, made by ITMCFM, can be found on the Centre's official website.

Much of the experts' attention was devoted to the FATF Global Network states' best practice in combating proliferation financing, including typologies for the detection and investigation of related crimes, national supervision, and examples of effective private sector engagement and outreach activities.

Another important aspect of the training concerned such issues as inclusion and exclusion of individuals and entities in/from the UN and individual countries' sanctions lists; confiscation; and freezing/unfreezing of assets of designated persons and entities.

However, the training was not limited to a theoretical discussion of the abovementioned aspects of CPF efforts, its participants were provided with the opportunity to apply knowledge in practice by completing a large block of practical tasks. Thus, to practice in building national-level coordination mechanisms, representatives of EAG member states took part in simulation exercises involving the adoption of new CPF legislation in a imagined country.

The teams of participants also tried to take their shot at identifying intermediaries and associates of persons from the UN sanctions list, and detecting and freezing their assets. During completion of this task, trainees simulated the decision-making process on providing the access to frozen assets.

The outcomes of these tasks were subsequently used by trainee teams to develop plans for CPF outreach to the private sector and preparation of guidance papers.

Summarizing course results participants highlighted the informative and interactive nature of the training, and thanked the organizers for the opportunity to put their knowledge into practice in the course of exercises designed to simulate real-life situations that representatives of national AML/CFT systems may face.

EGMONT GROUP FOCUSES ON FINTECH

The Egmont Working Groups and Committee meetings took place from January 27th to 31st, 2020 in Mauritius. Over 300 participants from FIUs, international organizations and observers took part in the event. The leaders of Mauritius highly esteemed Egmont Group activities and underscored the significance of the event

Inessa Lisina,
Deputy Editor-in-Chief

During the meeting of Information Exchange Working Group (IEWG) it was decided to concentrate its work on several operational projects with the aim to:

- effectively address the laundering of the proceeds of serious tax crimes;

- identify money assets associated with online sexual exploitation and abuse of children;

- establish and proactively disrupt large scale cross-border ML schemes (laundromats).

The IEWG members also discussed other ongoing projects and identified new areas of interest in order to effectively support FIU needs. The work includes detection of ML/TF risks which are related to the misuse of virtual assets and are characteristic to FinTech business models. IEWG started new work to identify Cyber-related crime typologies and risks in order to enhance FIU-FinTech cooperation and the role of FIUs for more effective recovery of criminal proceeds. Notably, the next Egmont Group meeting will focus on FinTech and its role in the FIU's activities.

The IEWG continued working on a number of key projects to combat ML/TF schemes. As part of the efforts to combat laundromats, the IEWG has developed indicators for testing using the FIU's real-time data to identify potential ML schemes.

As part of the asset recovery project, a decision was taken to create an electronic catalogue that will include data on the Egmont Group FIUs' powers regarding asset tracing, freezing of accounts and suspension of transactions.

The Membership, Support and Compliance Working Group (MSCWG) reviewed candidate FIUs' membership application from operational and legal perspectives.

The Policy and Procedures Working Group (PPWG) established and discussed recommendations to address existing impediments to information exchange between Egmont FIUs. Moreover, PPWG identified and defined terminology, which have conflicting interpretations when used by Egmont Group FIUs during information exchange.

The Technical Assistance and Training Working Group (TATWG) prioritized the topic of "Cryptocurrencies regulation and tracking by FIUs" for the training needs of Egmont Group members. TATWG will organize a training session on "Cybercrime and FinTech" during the Mexico Plenary meeting (July 2020).

Throughout the week, the Egmont Centre of FIU Excellence and Leadership (ECOFEL) hosted several workshops for participants of the meeting. Topics included issues of illegal wildlife trade and a presentation of ECOFEL's new eLearning platform.

All members of the Egmont Group expressed their gratitude to the staff of FIU of Mauritius – and especially its head Mr. Guillaume Ollivry – for high level of event organization.

As of January 26th, 2020, Mr. Mariano Federici`s (the head of FIU of Argentina) mandate as Chair of Egmont Group expired. The Egmont Group thanked Mr. Federici for his leadership during his tenure as Regional Representative for the Americas Region, Egmont Committee Vice-Chair and finally, as Egmont Group Chair. The Heads of FIUs appointed the Vice-Chair of the Egmont Committee, Mrs. Hennie Verbeek-Kusters (the head of FIU of the Netherlands), to act as Interim Chair until the end of the Egmont Group Plenary meeting in Mexico.

"ROLLING" AND "MIXER" CASHING-OUT: RECIPIENT COUNTERMEASURES

Dmitry Gronin,
Head of the Internal Control Service of Yandex.Money NBCO LLC,
member of the Compliance Council

The systematic approach to counter the most dangerous illegal schemes, including cashing out, demonstrated in the last years by regulators and participants of the financial market, leads to the fact that the interest of unfair market actors is shifted towards "rolling" and "mixer" schemes of dirty money transfer to a number of "straw men" recipients of funds on various fictitious grounds in small amounts in order to circumvent the control established by automated systems. Detection and suppression of these schemes become an actual task for the financial institutions serving individuals with the purpose of timely detection and suppression of criminal activities connected with tax evasion carried out by shell companies, illegal reception of budget funds, and also sale of illicit products (drugs, weapons etc.), various fraud and other schemes of illicit enrichment.

Yandex.Money, being a non-banking credit organization, operates under the license of the Bank of Russia and provides electronic wallet services to millions of its customers which are individuals. As in any modern bank, the simplicity and high speed of settlements, the remote nature of services require our credit institution staff to regularly study the actual illegal financial transactions typologies and develop compliance procedures, including the use of modern algorithms of machine learning, artificial intelligence and other automated facilities. These goals are achieved by implementing organizational and technical methods applied taking into account risk assessment not only of the customer, but also of banking products and services in the context of various channels of the addition to the accounts. The described approaches, in our opinion, are applicable not only to electronic wallets, but also to other financial products for individuals (bank accounts, payment cards, etc.), with the use of which assets may be received by the customer.

First of all, transactions involving direct crediting of funds from legal entities and individual entrepreneurs to individuals are subject to special control and restrictions.

The general technical solution to risk minimization in line of fictitious transfers is to introduce a limit on the allowable volume of direct crediting for a period of time to all wallets of the system from the external payer's account. The counterparty's taxpayer identification number (TIN) in an incoming payment order can be accepted as such banking information. The amount of funds received is determined by each identified TIN accumulated for the period. Corporate cards of a third-party payer are also subject to restrictions for crediting funds via payment system channels. Identification of the fact of using a corporate card can, with a high degree of reliability, be facilitated by the algorithms of analysis of a third-party card BIN/PAN code and the type of card product of a payment system (Financial Network Code), which are set up by the recipient's financial institution.

However, the application of limits and prohibitions alone would in some cases be an unjustified measure that did not meet the risk-based approach criteria. In order to credit customers (which are individuals) within higher limits framework, additional measures are required in respect of settlement participants, which can minimize the resulting risk. Such a tool may be contract practice on information and technological services for gathering, processing and transferring information about payments made directly with a third-party payer, which allows to grant it the status of a customer, carry out identification in due course, receive and analyze additional documents and information, establishing the business specifics, analyzing the customer's offer, the reasons for transfers and their relevance to the payer's scope of business activities and profile.

At present, the practice of mass registry-based payments is in great demand among legal economic entities. The experience of interaction with them has made it possible to generalize and classify a number of payment reasons, in respect of which it is possible to create methods and automated control tools to minimize the emerging risks of money laundering both at the moment of establishing business relations with a customer and in the course of his activity (see figure). At the moment of signing a payment agreement, the information on location, service points for individual customers, the number of persons on the staff of the organization or interacting with the organization under civil law agreements, accounting and tax reporting, applicable forms of agreements with an individual (standard-form contract, pattern, offer) is subject to

analysis. Depending on the payment reason and results of assessment of a payer's profile, including the use of scoring algorithms, a detailed adjustment of limits is carried out, and individual one-time, daily and monthly accumulation limits are used not only within the framework of a specific payment agreement, but also in the context of recipients.

The practice of identifying suspicious transactions shows that reasons which can be considered high risks are transfers for works/services under contractor agreements and agency contracts, return of previously received funds, settlements for sale of virtual assets and game content, insurance, charitable and other gratuitous payments. The aforementioned reasons for payments will require the application of additional approaches, for example, opening a bank account for the payer to be used as the main one, regular analysis of tax compliance, household expenses, and the counterparties' profiles.

Additional organizational procedures and requirements of acceptance for servicing have also been established for the acceptable risk payment reason:

1. Loans. Only microfinance institutions, pawnshops, and credit consumer cooperatives are accepted. The main reporting forms of the Bank of Russia with proof of submission marks are subject to analysis. The presence of the company in the register of the Bank of Russia and the absence in the regulator's negative lists are checked.

2. Fund income. Availability of a license of a professional securities market participant or other applicable license of a foreign jurisdiction is controlled.

3. Discounts and other compensation from the amount paid for the goods. The description of the process of selling goods and services, rules and conditions of providing discounts (compensations) to the buyer, a standard-form contract with the buyer is analyzed.

4. Bonus scheme (payment of bonuses and prizes at own expense, payment for surveys and quizzes, cashback services, other incentives for purchasing activity). The rules of carrying out an advertising campaign (award), establishing the procedure

for determining the recipients of incentive payments (rules for determining the winner), are analyzed. Contracts with third-party customers are to be provided. Availability of conditions in the contractual framework on performance of duties of the tax agent in relation to individuals - bonus payment recipients is controlled.

5. Payments of the intermediary platform for transactions of individuals. The rules of the platform operation are analyzed. Transactions are carried out with the opening of a nominal bank account to the intermediary platform, or with the receipt of documentary evidence that the platform used by a third-party bank account is nominal. Exclusion of "grey" payment flow is provided by the introduction of a unified technical identifier of the transaction of the seller and buyer, which ensures strict compliance with incoming and outgoing payment between the parties of the deal.
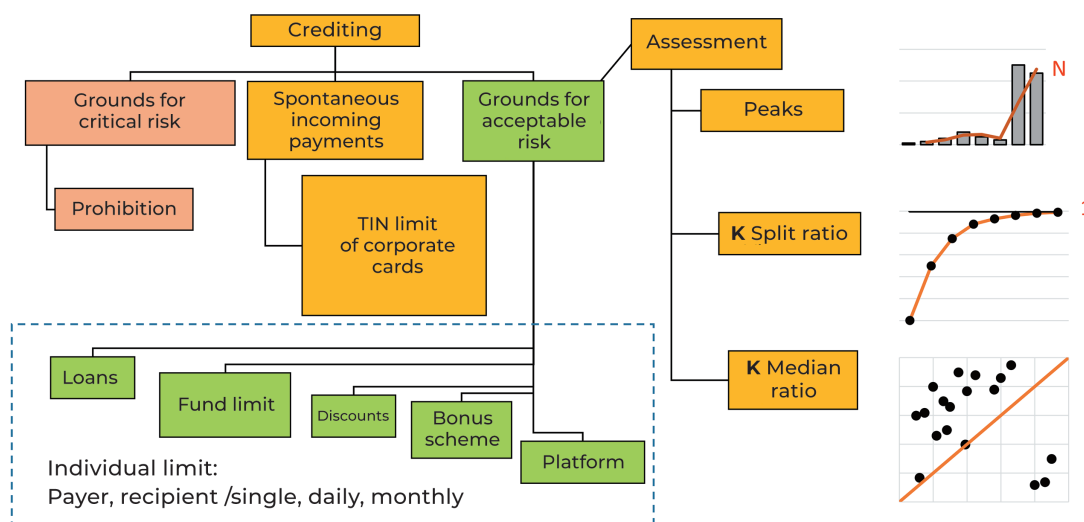
Monitoring of the volume and structure of actually performed transactions on a periodic basis serves the purpose of timely identification of changed payment behavior or non-compliance of payments with agreed reasons for them. When detecting a risky payment situation, requests are sent to the paying customers and documents are required to confirm the soundness of the payments made and their targeted nature. For example, for discounts and a number of bonus cases, documents certified by the executing banks confirming the fact of making a conditioned discount and real purchase bonus, as well as documentary

evidence of actual performance of tax agent's duties are provided. Cross inquiries are sent to natural persons - recipients of the largest payments, which allow to reveal the non-targeted nature of the payer's activity or contradictions in its argumentation.

To assess the risk of the payment state at the end of the control period, in addition to the fact that the total limit for the contract has been reached and the absolute values of the number and volume of payments have been made, the following indicators are used:

1. Peaks: share of the largest N bank details of recipients in the total volume of payments indicates the presence of the largest recipients, probably fictitious, standing out against the general background in terms of volume.

2. Split ratio: the ratio of the total amount of payments to the number of payment details of the recipients that are unique and to the amount of the established limit on the bank details. Raising of the coefficient from the lower grade to the value 1 indicates that the amounts of actual payments are consolidated in the area of established limits, which indicates the mass nature of splitting in order to evade the limit.

3. Median ratio: share of the number of unique bank details of recipients, which account for 50% of payments. It is also an indicator of unevenness of payments and the presence of the largest outstanding recipients (regardless of the setting value N. as in the indicator "Peaks").

Mass crediting management

More difficult to identify are "mixer" schemes associated with complex and confusing movement of dirty money on a long chain of accounts of "straw men". Such money enters the system as personal settlements. It becomes possible to reveal them with the use of both traditional periodic samples using mass and split criteria, and with the use of complex automated analytical systems based on machine learning.

Rapid response to the high-risk picture of revenue is provided by a specialized software package of "analytical machine", the result of which are both alerts sent to the compliance employees, and blocking operations of identified wallets including experts' analysis of the situation. Description and adjustment of rules and procedures of reaction of the analytical machine is made by staff of analysts of NBFI. Among the rules there are algorithms of linguistic analysis of the comment fields accompanying the operation, rules of identification of transit schemes characterized by the multiplicity of incoming and outgoing transactions with the details of individuals who are served by the NBFI and outside of it. "Mixer" schemes with a long chain are masked by their organizers by multiple breaking up and involving a large number of "straw men" - "drops". The "Fingerprint" technologies applied in the analytical machine allow to connect such persons into a single scheme, which allows grouping varieties based not only on personal data of clients, but also on other factors, such as coincident place and time of identification or card delivery, ATMs of sequential cash withdrawal, coincident IP-addresses and details of registration and remote access devices, regularities in other information traces left by the user of the applied software.

Regarding operations of the detected wallets, expert work on correctness of automatic classification of operations and profile is conducted. Requests are sent to the client and correspondence is carried out using a specialized software complex "Contact-Center", which provides a unified storage of client files and materials of in-depth verification. Expert processing of the results of the analytical machine operation provides machine training and facilitates fine-tuning of the applied algorithms. The said "expert-machine" system contains among other things, feedback, thanks to which the machine algorithms ensure the tracking of the stability of the payment behavior picture analyzed by the expert, in respect of which a positive evaluation was previously made, and identification of facts of its possible changes.

For the most critical identified factors, prompt responses are used, including termination of contractual relations and reporting (e.g. obvious text triggers, repeated use of previously identified and analyzed patterns, reliable third-party source information). With regard to the payment situation, where the compliance analyst can`t make an unambiguous and independent conclusion without additional information, enquiry messages are sent to clients and their documents and explanations are requested.

The application of these organizational and technical measures in the regulation and analysis of cash flow to the wallets allows quickly identify and prevent actions that have illegal activity features. At the same time, for example, prevention of shell microfinance institutions (MFIs) activities in a number of cases was carried out at an early stage - before negative information has been posted in their respect by the regulator and thus preventing and suppressing prohibited activity of fictitious MFI.

ASSESSMENT MODELS OF BANK CUSTOMER RISKS

The fight against money laundering and terrorist financing receives the increased nationwide attention both by the government authorities and private sector entities, i.e. business entities engaged in transactions with funds or other assets. Based on the outcomes of the recently conducted national money laundering risk assessment (NRA), the banking sector is placed in the higher risk category in view of its dominant role in the Russian financial system and broad versatility and wide accessibility of banking services, which makes credit institutions attractive to persons involved in money laundering schemes

Phillip Khyshiktuev,
Managing Director,
Head of Compliance Service
AO Raiffeisenbank
Member of Council
of Compliance

Maryana Zborovskaya,
Vice-President,
Head of Modeling Group
of Compliance Service
AO Raiffeisenbank

A rather large share of the informal ("shadow") economy and widespread use of cash still persists on the national scale, exploitation of shell legal entities, concealment of funds and assets obtained through crime committed abroad, and shortcomings of applicable legislation provisions aimed at preventing illicit withdrawal of funds abroad and cash-out schemes require from credit institutions to actively modify the approaches used for protecting themselves against money laundering threats.

If we look at the recent achievements in big data analytics, it becomes obvious that they offer significant opportunities for the application of statistical modeling methods for AML purposes. This article examines the experience of introduction and application of big data models for the compliance purposes, illustrated by the example of Raiffeisenbank.

Anti-Money Laundering Tools

When selecting tools for combating money laundering in practice, preference is typically given to the set of cost-effective tools and methods that allow to efficiently prevent damage at minimum expense. When it comes to prevention suspicious transactions in the bank, prompt assessment and identification of money laundering threats before onboarding new customers as well as before carrying out transactions for the onboarded customers allows to avoid damage that would otherwise be inflicted as a result of abuse of the banking services for illegal purposes.

The fact that a suspicious transaction has been carried out through the bank, even if such transaction is quickly identified in the process of the follow-up monitoring, shows that the damage caused by the transfer of funds to the recipient for their further laundering has already occurred. In order to mitigate the risk of bank involvement in illegal schemes in such situation, the toolkit that allows to quickly and accurately predict and assess the ML threats based on a large volume of data and to effectively implement adequate response measures, should be considered as an effective instrument for preventing suspicious transactions.

It is obvious that this task cannot be accomplished without adequate level of automation of the processes that allow to prevent, identify, assess and respond to the ML threats before the damage actually occurs.

In practice, the bank develops and implements the following set of consistent measures for addressing the mentioned task, that involves assessment of probability of carrying out suspicious transactions through the bank:

1. Identification of perspective customers posing the critically high risk, and enforcement of the legitimate right of a bank to refuse in onboarding such customers. On the one hand, this is the preventive measure that makes it impossible for such persons to carry out suspicious transactions through the bank. On the other hand, it establishes very high requirements for the quality of identification of such person – assessment of probability of carrying out a suspicious transaction by a particular person is conducted without analysis of his/her previous transactions (since no transactions have been carried by such person through the bank yet).

2. Prevention of carrying out suspicious transactions by current customers. This means that the customer is already onboarded by the bank, but for a number of reasons (described below) his/her transaction has become subject to monitoring before it is actually carried out. The decision as to whether or not to carry out an identified transaction is made by the analyst based on the results of scrutiny of such transaction.

3. Reduction of response time to unusual behavior of a customer identified in the process of follow-up monitoring of his/her previous transactions. Probability of customer involvement in ML-related activity is predicted with the application of the transaction models based on the array of static and dynamic data.

As regards to the first point, the following measures are taken in addition to the basic checks performed in the process of onboarding prospective customers:

- simple screening against the list of persons identified as posing the critically high risk;

- analysis of data for identifying the special criteria, which requires direct involvement of the analyst;

- verification of customer profile validity;

- scoring against the internal and external data.

It is noteworthy, that the manual verification of a prospective customer conducted by the bank employee allows to rely only on the formal indicators of potential involvement of the customer in ML schemes – in this case, risk assessment cannot be considered as sufficiently objective. Since the bank strives to minimize the risk of error in respect of each individual prospective customer, the application of statistical models allows to objectively assess ML risks posed by a customer and make the informed decision before establishing business relationships with him/her.

After a customer is onboarded, a new source of data – i.e. transactions carried out by him/her through the bank – becomes available for assessing the activity of such customer. It is the transaction data that are typically used for analyzing the existing customers, but the bank also takes into account information about individual customers received from different sources. The practice shows that processing and analysis of a combination of statistical and transaction data with the application of mathematical models gives the most accurate and objective result in respect of the existing customers.

As opposed to the follow-up monitoring, which is performed with the help of big data models with operational logic based on learning in the process of applying solutions to many similar tasks (i.e. machine learning), the real-time analysis involves the use of more simple rule-based logic and the predetermined parameters. In many typical cases that do not require manual handling of the model operation results, the special software applications automatically perform certain actions within the scope of the offered customer services (the so-called "robots"), are used to promptly respond to the identified threats in a timely manner. This approach allows the analysts to focus on truly complex cases and not waste time on obviously typical situations.

Model Range: Development and Success

Models for assessing risk of prospective customers

The AML requirements for the banks have been gradually enhanced over the recent years, which forces the banks to work more rapidly and rigorously, as time goes on.

Since the small and medium business segments are categorized as posing the highest risk, the bank actively develops the solution that will allow it to use the statistical models for assessing ML risks of prospective customers from these segments who seek to enter into the cash management and payment services agreement with the bank.

The practice showed that a combination of simple formal checks and screening model built on the bank internal statistics and supplemented by external data gave the most accurate assessment results.

Where could this model be used in the bank?

For example, for tackling decisions on opening bank account for prospective customer. The application of the statistical model in the process of follow-up monitoring of customer transactional activities (it is especially relevant at the initial stage, when the number of transactions carried out by a customer is still insufficient for objective analysis) significantly improved the monitoring quality. The model also demonstrated

its usefulness in the online monitoring scenarios, since it provides for more accurate assessment of risks associated with potential ML-related transactions taking into account the individual customer profiles.

At the very early stage of the development, the predictive performance of the model built solely on the bank internal data was analyzed. The main finding of this analysis was that even with the use of such laconic (limited) data the model can relatively accurately predict probability of carrying out suspicious transactions by a client if a bank account will be opened for him/her.

First practical steps aimed at implementing the statistical model in practice for assessing ML risks of prospective customers were made by the bank in 2016 – at that moment the model used only the internal data held by the bank.

However, in order to improve quality of the model built solely on the internal data, it was necessary to use some additional information.

A wide variety of external data sources was analyzed in 2017, and one of them was selected for practical use, which enhanced the model quality by over 10%. Such quality enhancement was due to the fact that external information about a prospective customer includes data that essentially differ from the internal data, which significantly improved the predictive performance of the model. It is worth mentioning another success factor of the new model: in parallel, the internal data processing algorithm was upgraded.

Additional analysis of a broad range of information sources conducted in 2018 identified another external data source, which intrinsically had medium performance, but still contributed to further improvement of the overall predictive performance of the model ensemble. In nominal terms, the predicative performance increased by over 5%, although such growth was partially facilitated by the fact that the model was once again updated.

In summer of 2019 we once again updated the model by incorporating additional data available within the bank and began to use external data more effectively, which resulted in further improvement of the predictive performance of the model.

In order to select the best model ensemble, we used the special metrics based on the business processes and actions triggered as the result of the model operation:

- in case of prospective customers posing the critically high risk – the bank uses the legitimate right to refuse to onboard such customers;

- in case of prospective customer posing medium risk – a bank account is opened subject to certain limitations in the scope of provided services;

- in case of prospective customers posing low risk – a bank account is opened under the regular terms and conditions.

Such approach obviously requires very precise differentiation between prospective customers who fall into the categories with the risk level other than low – for the low risk group, precise internal differentiation is not critically important.

To accomplish this task, the metric system was developed for assessing the accuracy of the model in lower range of the scores. Technically, a local score is determined based on the bank internal data by applying the logistic regression with L1 regularization, and the decision tree is used for assembling the scores. High results, along with maximum visibility and flexibility, prompted to choose this approach for practical application in future.

The model requires "careful treatment" and regular monitoring. The bank conducts monthly monitoring of the status and condition of the model to verify quality of its operation. If such monitoring reveals deterioration of the model performance, the model is reconfigured using new data.

It should be mentioned that it is very important to keep the accurate register of prospective customers rejected by the model. Since no actual transaction data of such rejected persons are available, the bank is unable to determine what percentage of transactions of such persons would be related to money laundering in case of their onboarding.

What way out of this situation can be suggested?

If it`s possible to select a group of prospective customers (the focus group) who received low scores that prevent their onboarding by the bank, and, despite such low scores, open bank accounts for this group of persons. After that, the actual behavior of the focus group will allow to assess the actual risk posed by the group members to the bank in general and compare this assessment with the expectations. If the expectations are met, it will indicate that the model is developed and implemented correctly.

Model for assessing risk of existing customers

As mentioned above, the scoring models built on transaction data, along with analysis of the customer files, are used for assessing ML risks posed by the existing customers.

Examined below are the specificities of models developed for assessing risk of money laundering by legal entities, individual entrepreneurs and natural persons, respectively.

Model for assessing risk of legal entities and individual entrepreneurs

In case of legal entities and individual entrepreneurs, the behavioral model has been developed which primarily analyzes the transactions carried out through the bank, while the data contained in the customer files are also taken into account for determining the scores.

The development of this model started with selection of the parameters (more than 150 indicators were tested), against which the customer activity is assessed in line with the guidelines and recommendations of the Bank of Russia, Rosfinmonitoring and the results of internal expert assessment. The selected indicators include tax burden, structure of payments broken down by types of business activity in general, parameters of individual transactions and other parameters that allow to assess whether or not the actual business activity is in fact conducted and if such activity is consistent with the applicable regulations and requirements.

The specialists possessing different expertise and skills, including AML analysts, model designers, etc., were involved in the development of the working set of parameters. The parameters were selected based on their statistical significance and contribution to the final model.

The behavioral model is a specificity that "looks" at general trends rather than at individual typologies, i.e. the model does not identify specific monetary movement schemes, but identifies, based on the aggregated parameters, those customers who carry out transactions probably related to money laundering.

Essentially, the model consists of two parts: the "slow" part that processes transactions carried out over a long period of time, and the "quick" part that looks at the most recent transactions. Such approach allowes to quickly and accurately enough identify suspicious behavior.

Based on the risk level and customer profile, the risky customers are divided into three risk groups in terms of probable: (1) cash-out transactions; (2) funds transit transactions; and (3) mixed transactions involving combination of the above. The specific measures are applied in respect of each of these groups, which minimize the risk of continuation and recurrence of suspicious transactions. As it was mentioned above, it is important to regularly monitor and verify quality of the model operation and to reconfigure it where necessary, since business entities find new ways of committing illegal actions and their behavior continuously changes and evolves.

Model for natural persons` risk assessment

On average, the level of money laundering risk posed by natural persons is lower compared to legal entities, but, in absolute terms, this segment includes a significant number of individuals who are involved in the ML-related illegal schemes.

With a view of identifying individual customers involved in ML schemes, the behavioral model was developed. This model also consists of two parts, the "slow" part and the "quick" part, as in case of the

model designed for legal entities. The "quick" part of the model includes several variables that were selected from the test group containing over 160 indicators. Similar to the legal entities behavioral model, most variables are related to customer transactions, but the data contained in the customer files also play the important role and are taken into consideration.

Based on the information on conducted transactions, the model places each active customer into one of the four different groups depending on probability of encashment and corresponding response measures taken by the bank.

Upon identification of the critically high ML risk, remote banking services provided to a customer involved in such transactions are promptly suspended. Transactions identified as posing the moderate ML risk are processed manually by the analysts.

It should be noted that simple knowledge of risks associated with a particular transaction is insufficient for placing the customers into different groups – for this purpose, the simple enough rules, based on customer behavioral pattern as well as on his/her background, and banking products are used.

Since autumn of 2019, the model has been completely reconfigured. To that end, the best existing variables were reassessed, and more than 100 new variables were introduced. This also included the application of more complex mathematical algorithms, namely the gradient boosting over decision tree ensemble. Verification of correctness of the relationships and partial interpretability of results were performed with the application of Shapley values used in the cooperative game theory. At present, the field tests of the reconfigured and updated model are underway.

***

As the regulator pays increased attention to the ability of banks to prevent suspicious transactions in advance trying to avoid damage, our bank focuses on application of the set of different tools that allow us to predict and, with high degree of probability, reliably prevent and disrupt attempts to carry out ML-related transactions through the bank.

It is important to note that the used scenarios are based on the guidelines and recommendations of the Bank of Russia and Rosfinmonitoring as well as on the internal statistics. The used models are primarily based on the internal statistics, but the bank additionally uses external data for assessing risk of prospective customers.

More complex approaches to modeling imply high standards and requirements for quantity and quality of data, but the end result is worth it. Besides that, all models require regular monitoring and updating for proper adaptation to the changing behavioral patterns of customers, the developments in the economy and, last, but not least, the information received from the Bank of Russia and Rosfinmonitoring. In the course of

monitoring, the bank assesses and reviews quality of its models on a monthly basis.

Apart from regular updating of the models, our plans for future includes search and analysis of new data sources, more detailed assessment of links and relationships of customers and further adoption of the online monitoring tools and robotization of processes.

And finally, we would like to emphasize the importance of international cooperation in fight against money laundering. Experience sharing at the international level allows to adopt best practices and helps to better understand and take into account the specificities of the national AML legislations of different countries in the process of establishment of AML monitoring system.

AML/CFT INNOVATION

USE OF ARTIFICIAL INTELLIGENCE ELEMENTS TO DEVELOP INFORMATION MECHANISMS FOR MONITORING PUBLIC PROCUREMENT OPERATIONS

Evgeny Loginov,

Doctor of Economic Sciences, Professor of the RAS, twice winner of the Russian Federation Government Prize in Science and Technology, Deputy Director of the Institute for Economic Strategies, Head of the Expert and Analytical Service of the Situation and Analytical Centre of the Ministry of Energy of the Russian Federation

Andrey Derkach,

Bachelor of the National Research Moscow State University of Civil Engineering

INTRODUCTION

The advantage of using artificial intelligence and Big data technology in the digital topology is the possibility to monitor the financial transaction chains in public procurement as a quasi-integrated information complex based on the integration of electronic trading systems.

On the basis of the artificial intelligence elements can be created the information base for monitoring resource and operating parameters of objects' operation in the "customer-supplier" system and their contractual interaction is created, offering wider and deeper possibilities of use of the agent-based modeling elements[1].

That is, there is a possibility to adapt the monitoring system in an automated mode to a complex system of orders and deliveries with a large component of information noise[2].

---

[1] V. Abramov. *State Procurement System and its structural and functional analysis* // Economics and business. 2016. No. 12-4 (77). PP. 497—504.

[2] E. Loginov, A. Matveev. *Increasing the efficiency of management activities of government agencies in the Russian economy on the basis of a network-centric information lattice of anti-shadow activities* // Economic Sciences, 2010, No. 70. PP. 32—39.

MULTI-OPERATIONAL INTERACTION OF DIFFERENT CATEGORIES OF OBJECTS (AGENTS)

The public procurement system is characterized by a large number of participants.

According to the data published on the website of the Unified Information System in procurement, in 2017 3,160,721 notices were published under 44-FZ and 223-FZ, in 2018 this figure was 3,231,786. It means that the number of published notices increased by 71,000 during the year. The share of macrocontracts in 2018 was more than 50% under 223-FZ and more than 30% under 44-FZ, which is mainly non-competitive purchases made from one supplier[3].

At the same time, in addition to direct state procurement, a large number of procurement operations in the country are carried out by companies with state participation and companies not directly related to the government order, but performing various functions of suppliers, subcontractors, etc. in the supply chain, the initial part of which is state or municipal procurement.

It is proposed to create an information-computational environment based on the possibilities of semantic analysis of data when placing and executing state orders of the relevant department based on the integration of information obtained from electronic trading systems (electronic trading platforms (ETP), etc.

In this case government contract is considered as a dynamic complex of multi-operational interaction of different categories of objects (agents) identified on the basis of direct or indirect participation in the use of the initial input of a certain amount of budget funds.

Semantic analysis of information resources received from electronic trading systems is carried out, where basic characteristics of support of a separate state contract (identified by a marker — a special unique number) and related thematic data are set. The analysis is carried out with the purpose of correlation of individual data of analyzed companies` activity cooperating in execution of government contracts through electronic trading platforms (ETP), comparing transactions dynamics with standard algorithms of financial assets dynamics (as well as prices, volumes of material resources, etc.) and their use in execution of similar government contracts. In the course of the analysis, the indicators characterizing the chains (matrices) of semantics of the analyzed links with respect to movement of financial assets and any other related indicators present in databases are identified.

Analytical services of such an environment should be integrated with monitoring services implemented by commercial banks that provide contract support and Rosfinmonitoring to adjust organizational mechanisms of financing and implementing state procurement. Descriptions of structured databases, consisting of various data obtained from electronic trading systems (prices for similar purchased materials, volumes of purchases of supplies in conjunction with earlier dynamics of current production activities and/or execution of similar orders, etc.), should be presented in a standardized manner using one of the acceptable formats and contain hyperlinks to financial and commodity transactions and participants of the cooperation.

Semantic links between any possible identifiable elements of state contract execution are presented as links between their descriptions and present themselves, as a rule, as a model of the subject area of database interaction, having the form of a directed graph, which, in its turn, may also be involved in other links.

---

[3] O. Tsyleva. According to the Chamber of Commerce and Industry of the Russian Federation, the Unified Information System operation in procurement requires serious improvement // https://tpprf.ru/ru/interaction/committee/kompurchase/news/294561/.

NETWORK CONVERGENCE OF ANALYTICS

This creates the possibility of convergence of the analytics by obtaining diverse data from ETP and from the largest possible number of any other data sources with correlation (or using agent-based modeling) analysis of the dynamics of the elements of execution of state contracts of different profiles (prices, payments, volumes of commodity resources, legal entities which are supply contractors, etc.) with the identification of matches or mismatches in the framework of explicit or brought to comparable criteria analogies.

This is the basis for identification of business agents' economic activity, where behavior of cooperation participants in public procurement (government contracts identified by markers) allows to identify the organizational strategy of a group of explicit and latent business agents and their characteristics (chronotype, participants, role-based structure, etc.). For example, analysis of business schemes with identification of relevant companies and assessment of their importance (correlation with the movement of financial assets or commodity resources) based on statistics of occurrence in other state purchases with different commodity or service profiles.

Structural links make it possible to detect identifiable elements in procurement operations dynamically localized as price, resource or any other matrices that formalize the information portrait of a state contract, using topical units of structured databases content consisting of various data obtained from electronic trading systems, as their different versions or thematic variants, typical or atypical, for example, an increase in purchases of specific types of services, despite the absence of a proportional growth of orders, which form the demand for such services.

It is possible to build vector models with the presentation of each studied order as a vector of weight coefficients of selected cases of price rise, which differs from the dynamics of inflation or price dynamics of groups of similar goods or their components in other purchases (for example, the inexplicable rise in price of products of individual enterprises, which is identified by converting the purchases in the framework of cooperation into a single scale of prices in the time and functional-order dynamics). It is possible to include here the analysis of balance sheets of companies[4].
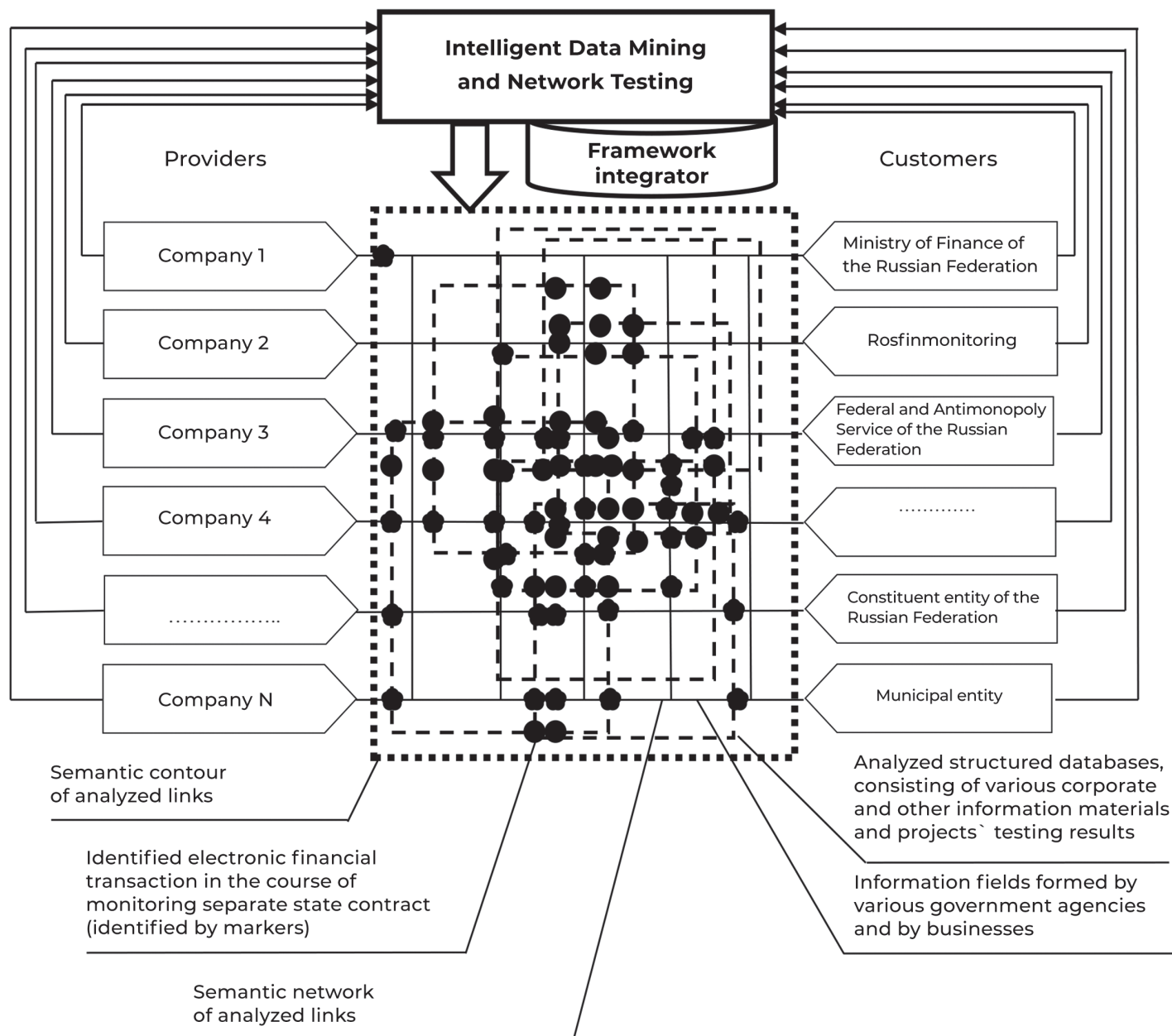
NETWORK-CENTRIC DATA INTEGRATION

As a result of the network-centric integration of data with spatiotemporal parameters binding within the framework of functional control and monitoring services, their components will be united by a given parameter into an observable quantity: for example, transferring of different characteristics of directly related, indirectly related and unrelated in an explicit form procurement groups into one comparable array with the detection of their previously hidden real dynamics (e.g. stability of participation of the same individuals [managers, owners of companies and others] in the key financial and economic operations carried out within the framework of a completely different, unrelated contracts).

It is necessary to finalize [on the basis of the most developed ETP] — with a view of qualitative increase of the control efficiency — a model [typical] pool of the interconnected information-analytical and computing services adapted to possibility of processing of various data received from electronic trading systems (ETP, etc.), and also from any other sources (Ministry of Internal Affairs, Central Bank of the Russian Federation, Federal Tax Service of Russia, Federal and Antimonopoly Service, etc.[5]. For example, databases of lost passports; shell companies; persons penalized under criminal or administrative law; managers or owners of companies that previously had large tax debts, performed large-scale offshore transactions, having minimal property assets, etc.).

---

[4] E. Loginov, N. Eriashvili, S. Bortalevich, A. Mikhailov. Monitoring of network links that identify the hidden beneficiaries of transactions in financial and property assets // State Service and Personnel. 2016. No. 2. PP 188—192.

[5] A. Ageev, E. Loginov, A. Raikov. Intellectual technologies of financial monitoring and control organization during the state procurement implementation // Economic Strategies. 2016. v. 18. No. 1 (135). PP 16—27.

Figure 1: Structural visualization of the semantics of analyzed links in the supply chain monitoring with state or municipal procurement as a starting point

Providers

Company 1
Company 2
Company 3
Company 4
……………..
Company N

Intelligent Data Mining and Network Testing

Framework integrator

Customers

Ministry of Finance of the Russian Federation

Rosfinmonitoring

Federal and Antimonopoly Service of the Russian Federation

………….

Constituent entity of the Russian Federation

Municipal entity

Semantic contour of analyzed links

Analyzed structured databases, consisting of various corporate and other information materials and projects` testing results

Identified electronic financial transaction in the course of monitoring separate state contract (identified by markers)

Information fields formed by various government agencies and by businesses

Semantic network of analyzed links

CONCLUSION

The Unified Information System created and developed by Rosfinmonitoring, as well as the Unified Integrated Data Transport Service that allows to ensure mutually beneficial use of information resources of government agencies and organizations to counteract illegal financial operations, should become the core of the system of coordinated management of information exchange.

BIBLIOGRAPHY

1. V. Abramov. State Procurement System and its structural and functional analysis // Economics and business. 2016. No. 12-4 (77). PP 497—504.

2. A. Ageev, E. Loginov, A. Raikov. Intellectual technologies of financial monitoring and control organization during the state procurement implementation // Economic Strategies. 2016. v. 18. No. 1 (135). PP 16—27.

3. E. Loginov, A. Matveev. Increasing the efficiency of management activities of government agencies in the Russian economy on the basis of network-centric information lattice of anti-shadow activities // Economic Sciences, 2010. No. 70. PP 32—39.

4. E. Loginov, N. Eriashvili, S. Bortalevich, A. Mikhailov. Monitoring of network links that identify the hidden beneficiaries of transactions with financial and property assets // State Service and Personnel. 2016. No. 2. PP 188—192.

5. O. Tsyleva. According to the Chamber of Commerce and Industry of the Russian Federation, the Unified Information System operation in procurement area requires serious improvement [Electronic resource] // https://tpprf.ru/ru/interaction/committee/kompurchase/news/294561/. (access date: September 26, 2019).

ROLE AND PLACE OF FINANCIAL MONITORING IN ECONOMIC SECURITY SYSTEM

Shamsiddin Allayarov,
Ph.D. in Economics,
Assistant Professor, Economics
Tashkent Financial Institute

Abror Mirziyaev,
Ph.D. Candidate
Tashkent Financial Institute

Growing instability of all processes in modern economic system indicates the increasing importance of adequate monitoring of the economic security management mechanisms in view of emergence of new large-scale political and economic risks, and also points to the ever-expanding role of the state in globalization era. For these reasons, enhancement of the economic security of a country at is pertains to the strategic deformation processes should be considered only in the context of a wide range of measures that include various elements and aspects of both domestic and foreign (international) economic activity.

The detailed analysis of the economic security definitions from various publications shows that many interpretations of this phenomenon are somewhat polarized and incomplete.[1]

Security is understood as the social state and living environment in which it and its structures, institutions and regulations exist, whereby they are able to persist in their essential characters under objectively changing conditions, and to independently and freely function consistent with their nature by neutralizing or eliminating any potential damage or harm, or adverse dynamics or parameters of the development.

Economic security is the field of science dedicated to the state of economy enabling rather high and stable growth of economic indicators; effective satisfaction of economic needs; state control over the flow and utilization of national resources; and protection of the country's economic interests at the national and international levels.

Economic security guarantees protection of the national interests. Its observation and preservation provide for proper operation of the government authorities, municipal institutions, business entities and organizations and promotes prosperity of individuals.

Economic security is not just a combination of factors that ensure stability, sustainability and economic growth-rate of a country. First and foremost, it constitutes the ground for normal and proper existence of human beings, society and state in

---

[1] Yu. Denenberg. *Methods of Conducting Financial Monitoring and Ensuring Economic Security of the Russian Federation* // International Student Scientific Bulletin, 2018, No.4-5; URL: http://eduherald.ru/ru/article/view?id=18957 (accessed on 06.11.2019)

general in the domestic and international environment. The level of economic security, being the regulating factor, characterizes the degree of development of the state as a whole. In the situation featured by active international cooperation, economic security is the top priority of the state, while economic security threats exist both inside and outside the country.

Economic security is the state of economy that provides for sufficient level of social, political and defence development and progressive evolution and ensures independence and invincibility of the country's economic interests to potential external and internal threats and impacts.[2]

At present, the following basic elements of the economic security system may be highlighted:

- forecasting social and economic development of a state in view of identified and potential factors and developments that pose threat to the economic security of a country;

- monitoring, including financial monitoring, and analysis of factors and developments that determine external and internal risks for the economic security of a country;

- development and implementation of response measures aimed at preventing the forecasted threats to the economic security at different levels of economy.

In order to ensure economic security, a variety of government enforcement and incentive measures are taken, and the special government authorities and agencies are established.

Economic security includes political, military, territorial, social, economic, foreign trade and other aspects. Due to its multifaceted nature, the economic security is the basis for the most important government functions and objectives.

Economic security can be achieved only following next conditions: the degree of dependence of the economy and escalation of domestic political, social and economic situation shall not exceed the threshold that poses threat to the national sovereignty, may significantly weaken the defence capabilities, entails sharp decline in the living standards and quality of life of the population, or may frustrate achievement of the global strategic goals of a country.

In this context, economic security of a country from the strategic viewpoint can be ensured only through implementation of a comprehensive set of measures covering a wide range of aspects of socio-economic live of the society pertaining to both domestic and international economic activity. Currently, the most important elements of the economic security system include[3]:

- forecasting social and economic development of the state in a view of identified and potential factors and developments that pose threat to the economic security of a country;

- monitoring and analysis of factors and developments that determine external and internal risks for the economic security of a country;

- development and implementation by the executive authorities of response measures aimed at preventing potential threats to the economic security of Russia in different industries and sectors of the economy;

- expert review of financial and business laws and regulations from the national economic security perspective.

At the modern stage of development, the following two ways of ensuring the economic security may be highlighted:

- ensuring macroeconomic stability through the application of, primarily, the economic and administrative measures, instruments and tools; and

- countering the negative developments, including crimes, underground market, etc., in the economy by implementing the law enforcement measures, including criminal intelligence, investigative and other techniques and tools for ensuring economic security.

---

[2] *Economic Security: Textbook for Universities*/ General Editors – L. Goncharenko and F. Akulin, Yurait Publishing House, Moscow, 2014, p.478.
[3] S. Gamonenko. *Financial Monitoring in the Economic Security System* // Memoirs of the Russian Academy of Business and Entrepreneurship, 2014, No.40. pp. 131-135.

The level of economic security is determined by a number of criteria, such as:

- geographical and geopolitical position of a county, existence of industrial and production facilities in its territory, and availability of natural resources and ability to extract and utilize them;

- level of economic development and defence potential of a country and its position in the international arena;

- support by the government of the industrial production sectors;

- development of competitive businesses;

- establishing parameters of the regional and sectoral level of GDP;

- availability of strategically important material resources stock in case of emergency.

It is important to understand that economic security is not the completely independent and self-contained element. With the development of external economic relations and growth of foreign trade, the economy of each country is dependent, to one degree or another, on economic security of other countries and international communities. In this situation, it is critically important for a country to develop its own competitive production industry that will enable it to profitably operate in the international market as an equal partner.

It is not the current performance indicators, but the threshold parameters that are indicative of the level of economic security. Indicators are the limits, failure to adhere to which hinders the normal course of evolution of the reproduction process elements and triggers negative and destructive trends that are harmful for the economic security. For example, these include numerical or percentage rates of social security, unemployment, education, inflation, taxation, etc.

When these thresholds are nearly reached, it gives rise to the factors that threaten the economic security, and if they are exceeded, it triggers economic crisis of decline.

The efforts undertaken by the government for ensuring economic security include a number of elements:

1. monitoring, including financial monitoring, for identifying potential sources of danger and further origins of threats;

2. development and legalization of measures aimed at preventing the emergence of threats and their elimination;

3. translation of these measures into reality, i.e. implementation of the response measures for eliminating economic threats.

Thus, the goal of development of the economic security system on the one hand, is to create the environment that would ensure stability of the national economy in the situation featured by highly uncertain international, social, economic, political and other factors, promote sustainable development of the Russian economy, and provide the adequate living standard and decent quality of life of the population, and, on the other hand, it should protect the economy against threats posed by the perpetrators of economic offences by way of combating the economic crime, inter alia, through implementation of preventive measures and elimination of causes and conditions that give rise to such criminal offences.

As the globalization processes have become more intensive, the government authorities responsible for the economic security encountered the problems related to increasing volumes and accelerated speed of information flows in the global economic system. And this implies the need to analyze and timely assess the information about the state of the national economy, regional economies and the global economy and forecast the dynamics of the economic processes and developments. Without these measures, it will be impossible to make correct decisions in the economic sphere, inter alia, for ensuring the economic security, forecast the critically important parameters of social and economic development and select the adequate tools for enhancing economic security. In this context, it is expedient, in our opinion, to consider the potential of financial monitoring that can enable the government authorities to have the clear picture of economic activity and, at the same time, can be used as a tool for conducting financial oversight.

The systemic task of a state in the competitive economy is to counteract challenges and threats emanating from the external (posed by the global economy or the non-economic methods used by is stakeholders) and internal environment and to enhance stability of the national economic system.

Reduction or complete disengagement of the government from many areas of the society activities generates economic risks (threats) in the short and long-term perspective. This applies to a wide range of the social and economic sectors that play the decisive role in the economic development and include the public, industrial, structural, regional and economic policies. It seems fair to say that this gives rise to strategic and tactical threats to the economic security.

The national anti-money laundering and counter-terrorist financing system is the important element of the economic security system. Money laundering means the activity carried out for concealing the source and origin of funds or criminal assets and giving the appearance of legitimacy to their source in order to avoid the law enforcement suspicions and prevent tracing and detection of the crime proving evidence.

The effective use of the public funds and material resources is the prerequisite for enhancing the economic security and complete implementation of the social and economic programs. At the same time, the economy currently suffers significant losses as a result of non-compliance with the financial and budget discipline. Misuse, fraud and direct embezzlement of public resources, illegal transfer of funds abroad and money laundering have become a common practice today. The number and total amount of committed financial breaches and offences has not declined in recent years.

Negative processes in the economy are, to a large extent, caused by the weakened public governance and administration framework, which includes less stringent government financial oversight, and also by insufficient scientific exploration and refinement of new market mechanisms, including the finance, loan, taxation and other instruments.

The need for reforming and upgrading the government financial oversight system has become obvious and is acknowledged by the legislative and executive authorities. However, adoption of the well-grounded and adequate decisions for restructuring of this system requires thorough scientific research and exploration of a wide variety of issues, including those pertaining to implementation of government financial monitoring as the most important tool for ensuring economic security of the society.

In the present situation, one of the approaches to improvement of the government financial monitoring involves its treatment as one of the elements of the public governance and economic security mechanism.

In these circumstances, the development of thoroughly elaborated recommendations for improvement of the government financial monitoring and enhancement of its effectiveness in the economic security system can be considered as the pressing theoretical and practical problem.

Financial monitoring is the basis of economic security which lays the foundation of determining the level of economic development of a country and underpins improvement of economic performance and economic growth.

Establishment of market relations and emergence of joint stock companies, leasing companies, commercial banks and other business entities typical for the market economy required fundamental restructuring of the financial monitoring system.

Active development of the Internet resources, introduction of international foreign currency accounts and enhancement of the government anti-corruption and counter-terrorist financing programs make this type of economic monitoring ever more important and relevant. Extensive use of data obtained through monitoring will facilitate and expedite solution of many pressing problems especially in remote regions.

Although the financial monitoring institute has been, to a large extent, introduced in the anti-money laundering and counter-terrorist financing laws and regulations, this does not preclude the possibility of its application in other areas of financial and economic activity.

Scientific views on the essence of the "financial monitoring" concept demonstrate the multiplicity of tasks and objectives that can be pursued with the application of this tool for ensuring economic security of a country. Financial monitoring is a part of the general national financial security mechanism and the information and analytical system intended for examining changes in the performance indicators that help to assess the degree of economic security of a country. Financial monitoring is a complex of methods and tools designed for collecting, processing and analyzing data and diagnosing the dynamics of various economic processes, operations and developments, which is used in multiple areas of economic security for both assessing the state of the economy of a country or a region and identifying factors facilitating economic crime.

Thus, financial monitoring is a combination of methods, techniques and tools designed for collecting, processing and analyzing information and forecasting the dynamics of all economic processes, operations and developments, which can be used in various areas of economic security for both assessing the state of economic security of a country or a region and identifying factors facilitating economic crime as well as for combating these criminal offences, including money laundering offences.

The use of financial monitoring for the economic security purposes will significantly facilitate accomplishment of many tasks related to detecting and counteracting the security threats. It will allow to identify the threat sources, and prevent their further expansion. And in case of emergence of large-scale external or internal threats, the well-established and robust monitoring system will help to determine, as accurately as possible, potential consequences, eliminate them and prevent recurrence of such situations in future.

The anti-money laundering and counter-terrorist financing institutional structure is composed of two core elements that differ in terms of the parties involved and the missions assigned to them, namely: law enforcement block and financial monitoring. The financial monitoring element can be further divided into two levels: initial financial monitoring and state financial monitoring.

Tashkent Financial Institute

The subject of the initial financial monitoring is the entities that conduct transactions with funds or other assets, and other entities and persons specified in the legislation, whose obligations include, among other things, customer due diligence, identification of suspicious transactions and reporting such transactions to the designated government authority. The state financial monitoring is performed primarily by the designated agency that oversees financial transactions based on information received from the obliged entities, verifies the received information and disseminates findings to the law enforcement agencies when there are sufficient grounds to do it.

Monitoring is performed by collecting, systematization and analyzing information and incudes development of recommendations and directives based on the results of conducted examination and analysis.

Financial monitoring is conducted by analyzing the economic security parameters, which include nearly 150 indicators, such as GDP volume, gross crop yield, unemployment rate, inflation rate, foreign debt, gold and foreign-exchange reserves, budget deficit, ratio of food imports, etc.[4]

Apart from the indicators themselves, the important role is played by the economic security indicators. These are the instruments that represent the qualitative characteristics and determine the boundaries between safe and dangerous developments in

different sectors of the economy. Financial monitoring involves comparison of the quantitative values of the indicators and their threshold parameters. This diagnostics answers to the questions, such as: what sectors of the economy have entered into the "dangerous zones"; what is the extent of their exposure to danger; where and in terms of what indicators the existing threats most seriously affect the economic interests of a country?

Financial monitoring as a method of continuous monitoring and analysis of financial flows, is one of the tools used for counteracting the aforementioned developments and problems they entail, which allow to identify the causes of crime. Such monitoring involves not only recording and analysis of already committed breaches and offences, but also allows for identifying the most probable breaches that may occur in future.

Not just simple collection of data and indicators, but also monitoring of their dynamics and determining statistical pattern and relations among them are

the fundamental prerequisites for adequate and successful monitoring.

Monitoring is the multistep process. At the first stage, the designated authorities should be appointed, the relevant monitoring criteria and their respective values are determined, and the convenient assessment scale is developed. The next stage involves collection and distribution of information, where all collected data are transmitted to the monitoring center. After that, analysis is conducted, in the course of which the factors that have positive and negative impact on the economic security of a country are identified. Then, the action plans are developed for eliminating the dangerous factors and preventing their further recurrence. At the final stage, the achieved results are summarized and the relevant directives, recommendations and plans are developed.

In summary, it can be concluded that financial monitoring is the important tool available to a state for performing its economic security control functions.

---

[4] M. Proshunin. *Financial Monitoring: Subjects, Objects and Importance* // Bulletin of the Peoples' Friendship University of Russia, Legal Science Series, 2008, No.2, pp.43-80

INFORMATION RESOURCES

A SERIES OF VIDEOS ON TOPICAL AML/CFT ISSUES IS POSTED ON ROSFINMONITORING WEBSITE

Anna Bulaeva,
Reporter

With the view to enhance the efficiency of the work conducted by the AML/CFT experts, the International Training and Methodology Centre for Financial Monitoring produced a series of videos. The State Secretary, Deputy Head of Rosfinmonitoring, Pavel Livadny, who held this position from August 1, 2013 to February 6, 2020, acted in the capacity of a lecturer.

The videos start with the panoramic view of the Academician Sakharov Avenue in Moscow and the facade of the Rosfinmonitoring building, and then show the building interior, including the spiral staircase and the conference hall of the Russian Financial Unit Headquarter. In the conference hall, the main actor starts his work, namely prepares presentations of the topics covered by the videos.

The first video is dedicated to the national and sectoral money laundering and terrorist financing risk assessments in the Russian Federation. The content includes the definitions, risk assessment levels, information resources used to inform the private sector about NRA results, and the money laundering and terrorist financing methods and transactions that pose the highest risk. The results of the national risk assessment assisted in development of the Interagency Action Plan for mitigating the identified ML/TF risks. The NRA findings are currently used in practice by many representatives of the private sector and self-regulatory bodies for assessing risk of their customers, products and services and developing risk management policies.

The second video, which highlights the key issues related to combating the financing of proliferation of weapons of mass destruction (CPF), presents the current mechanism of implementation of the relevant UN Security Council Resolutions, including targeted financial sanctions, and the CPF measures.

Production of series of videos in Rosfinmonitoring Conference Hall

The third video covers the relevant challenges related to ML/TF risks management when providing services to politically exposed persons. The main goal of managing the ML risks in the course of maintaining business relationships with politically exposed persons is to apply preventive measures in case of detection of corruption-related risks. The video clarifies in detail the concept of a PEP (politically exposed person), who is defined by the Financial Action Task Force (FATF) as an individual entrusted with prominent public functions. The legislation of the Russian Federation requires the obliged entities to take measures in respect of PEPs for managing the related ML/TF risks and, therefore, Rosfinmonitoring develops and issues the relevant methodological guidelines and information letters.

The videos posted on Rosfinmonitoring official website are demonstrated in the course of AML/CFT events and help to enhance effectiveness of implementation of the AML/CFT preventive measures.

NEWS

ITMCFM Updated Electronic Training Courses

Following the revision of the international and national AML/CFT legislation, the International Training and Methodology Centre for Financial Monitoring updated the electronic training courses *"Ad hoc AML/CFT Training", "Roles of Organizations in Combating Money Laundering and Terrorist Financing", "International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation (FATF Recommendations)"* and *"Methodology for Assessing Technical Compliance with the FATF Recommendations and the Effectiveness of AML/CFT Systems"* posted in the Self-Education section of the Personal Account on Rosfinmonitoring website.

The use of the electronic training courses allows for:

- Arranging remote training and follow-on testing of knowledge received in the process of training by employees of entities engaged in transactions with funds or other assets;

- Meeting the demand of AML/CFT specialists in educational services for development of the basic knowledge, skills and competencies required for further effective work.

Electronic Training Courses Developed by ITMCFM for the Russian Federation

Autonomous Non-Profit
Organization ITMCFM

2020