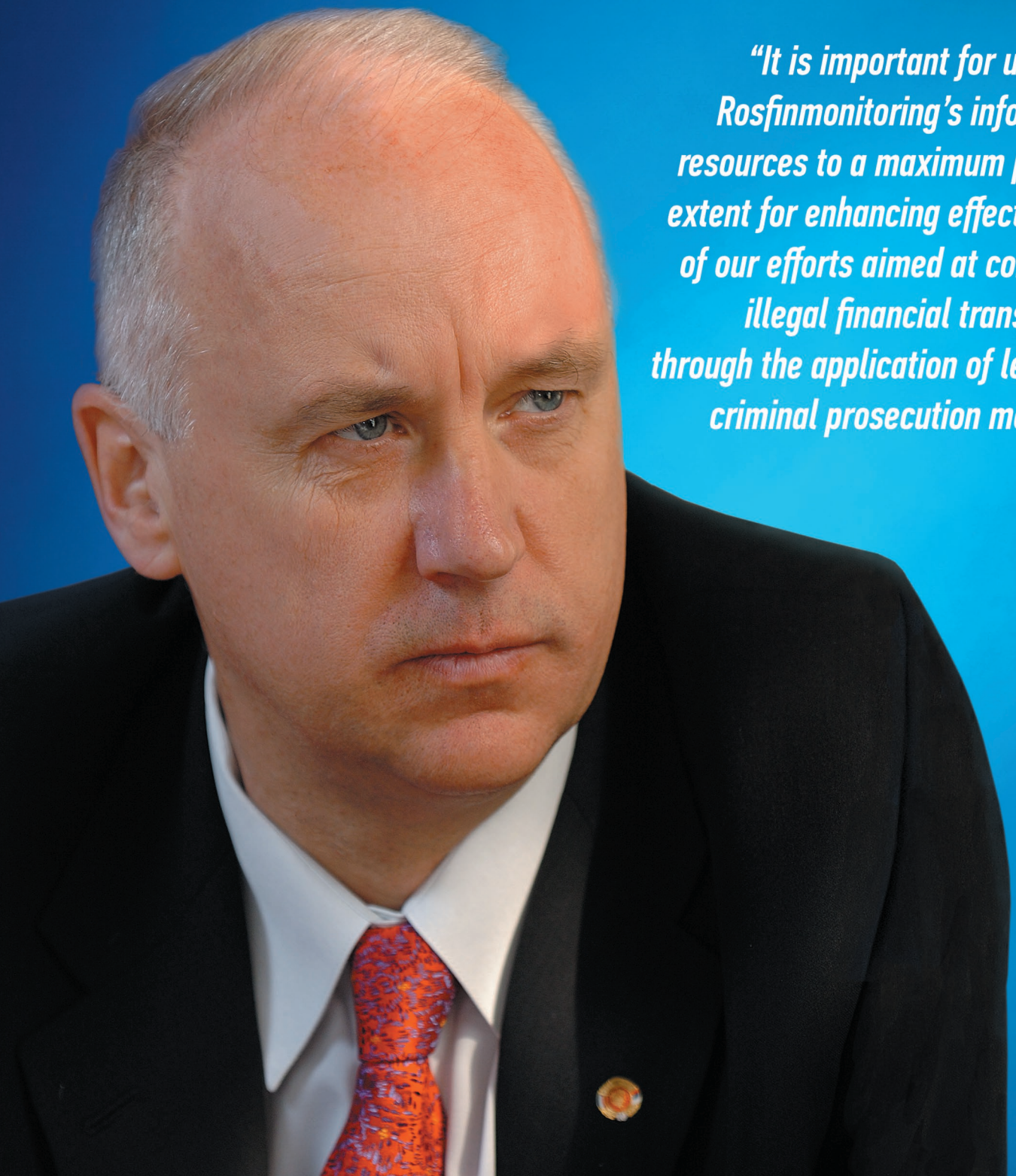
FINANCIAL SECURITY

NO. 7 DECEMBER 2014

A. I. BASTRYKIN:

"It is important for us to use Rosfinmonitoring's information resources to a maximum possible extent for enhancing effectiveness of our efforts aimed at combating illegal financial transactions through the application of legal and criminal prosecution methods".



FINANCIAL SECURITY

CONTENTS

EDITORIAL BOARD

Chairman of Editorial Board

Yu. A. Chikhanchin

Deputy Chairman of Editorial Board

V. V. Ovchinnikov

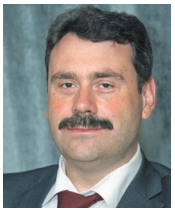
MEMBERS OF EDITORIAL BOARD

Yu. F. Korotky

G. V. Bobrysheva

V. I. Glotov

A. S. Klimenchenok



P. V. Livadny

V. P. Nechaev

A. G. Petrenko

A. N. Frolov

DEAR READERS!

This is the final issue of the *Financial Security* journal in 2014.

It was a very tough year for all of us. It began with the Olympic triumphs in Sochi in February and the reintegration of Crimea in March, but it ends with international sanctions and mounting economic challenges. In June Russia passed the presidency of the FATF to Australia at a ceremony whose venue, contrary to the original plan, was moved for political reasons at the request of some countries from Moscow to Paris. Back then, we once again reminded our Western colleagues that FATF is a purely technical mechanism established to combat money laundering and terrorist financing challenges and therefore should not be used as a forum for settling political scores. Fortunately, the international AML/CFT community took note of Russia's position.

In autumn, our country succeeded in presenting its third follow-up report at the Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL). Despite the external political factors, MONEYVAL's approach to the discussion of our report was objective and unbiased. The country's serious efforts aimed at bringing its AML/CFT law in line with international standards undertaken over the recent years received a positive assessment of the European Community.

This year also saw the Russian Financial Intelligence Service, just like the country as a whole, move to a new level by assuming in our case a raft of new powers, including control over the account transactions of the strategically important for the national economy enterprises. Our Risk Assessment Centre has begun working at full capacity, and is already starting to find its customers. The new challenges facing Rosfinmonitoring were outlined by the President of the Russian Federation in his annual address to the Federal Assembly.

«Inappropriate use or embezzlement of budget allocations for state defense orders should be considered a direct blow to national security. We should deal with such manifestations in the same way we deal with terrorist financing,» said V. Putin, instructing Rosfinmonitoring and other structures involved «to work out a system of tough operational control over the use of resources from state defense orders.»

In the context of the evolving international political and economic environment as well as the existing and future sanctions against a number of countries (including Russia), the risks and threats to the national anti-money laundering system, both at the international and national levels, increase dramatically.

The challenges outlined by the country's leadership coupled with the above risks and threats force and oblige us to rethink our approaches, improve performance as well as more clearly define the goals, ways to achieve them and the expected result. It's necessary to improve efficiency of our work.

In addition to the tasks that are already being addressed by us, we need to find our place in the evolving mechanism of state control, quickly identify the existing risks and threats and, in conjunction with the relevant ministries and departments, take whatever steps necessary to eliminate them.

All results should be put into concrete figures to allow us to see progress more clearly. The effectiveness of our activity must be expressed in:

- prevention of misappropriation, especially of budgetary funds;
- decriminalization of the economy and financial institutions.

Whatever the political situation, Russia, as always, will remain committed to fighting financial crime.

I wish all of us to be successful at tackling the new challenges in 2015!

Happy New Year!

Rosfinmonitoring Director
Yury Chikhanchin

COVER STORY

THE FEDERAL FINANCIAL MONITORING SERVICE AND INVESTIGATIVE COMMITTEE OF THE RUSSIAN FEDERATION: TOPICAL ISSUES OF INTERAGENCY COOPERATION

A joint meeting of the executive councils of the Investigative Committee of the Russian Federation and the Federal Financial Monitoring Service was held on September 23, 2014

Irina V. Ivanova,
Chief Editor

The event was attended by members of the executive council of the Russian IC, heads of departments of the central office and criminal investigation departments in the Federal Districts of the Russian Federation, heads of Inter-regional departments of the Federal Financial Monitoring Service, as well as invited guests.

In his opening remarks, Yury Chikhanchin, Director of Rosfinmonitoring, recalled last week's successful report to the Council of Europe on compliance of the Russian anti-money laundering system with international standards. Among the key factors contributing to the positive assessment of the AML/CFT systems by the international community are the regular updating of information resources and automation of processes primarily aimed at increasing the transparency of financial institutions. This approach, according to the head of the country's financial intelligence, will also help countries intensify their fight against corruption, which is particularly relevant given the existing requirement for financial institutions, besides submitting suspicious transaction reports, to identify transactions involving the so-called VIP persons.

«VIPs are those who affect the economic and political situation in the country,» reminded Yu. A. Chikhanchin, noting that the majority of financial institutions in Russia maintain similar lists and compile data on revenues and expenditures of such persons.

Alexander Bastrykin, the Chairman of the Investigative Committee, spoke of professionalism of the Rosfinmonitoring staff that allows the Investigative Committee to obtain high-quality materials used in the criminal proceedings against embezzlers of budget funds.

Speaking of the anti-corruption efforts, the IC chairman drew attention to the fact that «*the growing number of corruption cases necessitate not only the use of punitive but also well-calibrated legislative measures*». In this regard, Alexander Bastrykin recalled the legislative initiatives of the Investigative Committee in the field of deoffshorization of the economy, in particular, the draft law on the introduction of criminal liability of legal persons to encourage the repatriation of criminal capital siphoned out of Russia and invested in foreign companies.

During the joint meeting of the executive councils, participants discussed topical issues in interagency cooperation, including the coordination of joint actions of the investigative authorities and Rosfinmonitoring departments in the Federal Districts of the Russian Federation, and spoke about ways to improve the existing anti-corruption and anti-money laundering legislation.

Yury Chikhanchin:

If we look closely at the text of the Presidential Address to the Federal Assembly, we will see that among the key objectives for the planned period are:

- increasing transparency of financial institutions;
- increasing transparency of the real economy.

Indeed, if these sectors become transparent for the state, then for the entities handled by the Council would be quite difficult to carry out their criminal activity.

The attainment of this goal depends on the efforts of both Rosfinmonitoring and the Investigative Committee.

If we look at the issues of interaction between our two agencies, several of them stand out:

- the work on specific cases aimed at identifying and documenting the financial and economic components of corruption, including participation in the search for assets and seizure of criminal proceeds;
- the preventive work aimed at identifying corruption risks in different sectors of the economy;
- legislative efforts aimed at addressing the identified shortcomings exploited by corrupt officials.

... The effectiveness of our joint work should be measured not in the number of cases, but in our ability to create and improve an effective anti-corruption system and, if necessary, in recovering the stolen from the state and private owners assets. All this will allow us to achieve our goal: to reduce the level of corruption in our country.

IT IS IMPORTANT FOR US TO USE ROSFINMONITORING'S INFORMATION RESOURCES TO A MAXIMUM EXTENT POSSIBLE

Alexander I. Bastrykin,
Chairman of the Russia's Investigative Committee

At the joint meeting of the Russia's Investigative Committee and Rosfinmonitoring held with the purpose of finding the ways to improve effectiveness of our mutual cooperation, we discussed a wide range of anti-corruption and anti-money laundering issues that were within the shared competence of our agencies. We discussed practical aspects of our collaboration and the encountered challenges, shared the best practices and experience as well as worked out further steps for enhancing effectiveness in such an important objective of the national policy.

The issues discussed at this meeting are of great importance since, in the context of the current large-scale economic reforms, the robust mechanism of our cooperation will serve as the reliable safeguards against possible misappropriation of budget funds allocated for implementation of the national projects of the highest priority.

The Investigative Committee uses the information disseminated by Rosfinmonitoring and the Accounts Chamber of the Russian Federation for investigating the most complex corruption-related criminal offences committed in connection with public procurement contracts in the housing and public utility, education, public health and other critically important sectors of the national economy.

Alexander I. Bastrykin

This allows us to focus, to the maximum possible extent, our efforts on combating corruption and to assess the financial damage suffered by the state as a result of these criminal offences.

The hard work meticulously performed by financial intelligence officers and investigators should ultimately be aimed at identifying and prosecuting all types of embezzlers of budget funds.

High capacity of the Federal Financial Monitoring Service to pursue this goal in proven by the fact that, at the Plenary Meeting of the Egmont Group (with membership of 140 FIUs) held two years ago in St. Petersburg, Rosfinmonitoring won the Best Egmont Case Award competition.

In this context, it is important for us to use Rosfinmonitoring's information resources to a maximum possible extent for enhancing effectiveness of our efforts aimed at combating illegal financial transactions through the application of legal and criminal prosecution methods.

It should be noted that we have already gained positive experience of cooperation and coordination in this area. Our joint efforts resulted in disruption of multiple misappropriations and embezzlements in course of sales of real estate property, land plots and stock owned by the companies and organizations controlled by the Ministry of Defense of the Russian Federation.

For example, based on the information and materials provided by Rosfinmonitoring the investigators of the General Military Investigation Department of the Investigative Committee instituted criminal proceedings against the senior managers (Alexander N. Yelkin and Yulia V. Rotanova) of "Slavyanka" housing and utility company affiliated with the Ministry of Defense of the Russian Federation for committing exceptionally large-scale fraud, receiving bribes and laundering over 600 million rubles of illegal proceeds.

And this is just one of many examples of our successful cooperation.

Currently the court proceedings are underway against the former head of the Property Department of the Ministry of Defense of the Russian Federation (Yevgenia Vasilyeva) and other high ranking officials charged with exceptionally large-scale fraud, money laundering, abuse of office and abuse of powers granted to them for discharging the business management functions. A total losses and damage inflicted by the criminal activities committed by the organized group that sold the Ministry of Defense property and stock at deliberately low prices exceeded three billion rubles.

Besides that, the joint efforts of our agencies resulted in disruption of multiple misappropriations of budget funds and further laundering of criminal proceeds in connection with public procurement contracts in the housing and public utility, road construction and public health sectors. (Those cases included, in particular, misappropriation of budget funds allocated for procurement of tomographic scanners under the National Health Program, where information and materials provided by Rosfinmonitoring were used for conducting investigations and instituting criminal proceedings against several heads of the regional public health departments who were involved in embezzlement of budget funds).

Since the establishment of the Investigative Committee, it filed with the courts over 30 thousand corruption-related criminal cases, although, we clearly understand that this figure is the far outcry from what we strive to achieve. Therefore, there is no need to explain that in order to effectively fight the surging corruption wave it is necessary to impose not only criminal sanctions but also to implement targeted legislative measures.

In this context, the Investigative Committee has prepared proposals for "de-offshorization" of the Russian economy. These initiatives are primarily aimed at combating illicit capital outflow from Russia. At the same time, we clearly realize that legal capital flight shall be prevented only by applying the appropriate economic measures, such as creation of a congenial investment climate, improvement of the legal framework, protection of private property and implementation of flexible tax policy.

We propose the following basic measures for illicit capital flight repatriation and prevention of further "offshorization" of the economy.

1. Abuse of the right shall be explicitly prohibited by the tax and levies legislation. This measure will help to prevent aggressive tax planning which involves artificial structuring of transactions and company groups in such way that the main portion of various taxes is levied upon foreign companies or upon tax exempt domestic companies, which ultimately pay no taxes at all.

This initiative was supported by the Chair of the State Duma Committee on Budget and Taxes (Andrey M. Makarov) who introduced the relevant bill (draft law No. 529775-6) into the State Duma.

2. The Chair (Valentina I. Matvienko) and other members of the Council of Federation have introduced the bill that extends the list criminally punishable methods of tax evasion through providing false (or concealment of) information about controlled foreign entities.

3. Possible imposition of criminal liability on legal entities in Russia is being extensively discussed and examined now. This measure will lay the effective legal foundation for extraterritorial criminal prosecution of not just natural but also legal persons and will allow for repatriating criminal capital that has been illicitly withdrawn from Russia and placed on the foreign companies' balance sheets. Currently this process is impeded by the fact that such prosecution requires dual criminalization of offence, including dual criminality of perpetrators in both cooperating countries. However, only natural persons are currently held criminally liable in Russia.

This measure will also allow for prosecuting foreign credit institutions that facilitate illicit capital outflow from Russia and conceal information about Russian-resident beneficiaries of financial transactions from our law enforcement agencies.

I express gratitude to Rosfinmonitoring for conceptual support of the bill on imposition of criminal liability on legal entities drafted by the Investigative Committee.

At present, this bill is also supported by the Central Bank, the Federal Service for Fiscal and Budgetary Supervision, the Institute of Legislation and Comparative Law under the Government of the Russian Federation, the Financial University under the Government of the Russian Federation and by other agencies and organizations.

Following the extensive discussions, a number of important decisions were made at the joint meeting of the boards of the Investigative Committee and Rosfinmonitoring. In particular, it was suggested that the heads of the Investigative Committee departments and the heads of Rosfinmonitoring structural divisions should:

- More actively use the mechanisms of identification, seizure and confiscation of proceeds from criminal offences punishable under Articles 174 and 174.1 of the RF Criminal Code (Article 104.1 (1) (a) of the RF Criminal Code);
- Take measures to ensure wider application of proactive approach to identification of suspicious transactions in order to establish grounds indicating that a transaction or deal is related to ML or FT and reporting such transactions (deals) to the investigative departments of the Investigative Committee.

Besides that, the relevant departments and divisions were tasked with:

- Considering the legislative initiative regarding introduction of amendments to Article 151 of the RF Criminal Procedure Code so that investigation of criminal offences punishable under Articles 174 and 174.1 of the RF Criminal Code will fall within the competence of the Investigative Committee;
- Preparing proposals on improvement of the mechanism of identification of laundered funds and other assets obtained in a criminal manner and their seizure for further confiscation or compensation of losses.
- Developing a draft agreement on cooperation between the Investigative Committee and Rosfinmonitoring;
- Preparing training programs (taking into account the facilities and capabilities of the International Training and Methodology Center for Financial Monitoring under Rosfinmonitoring) to be incorporated into the educational process, and also programs of AML workshops for the officers of the Investigative Committee.

I am convinced that we will deepen and extend our successful coordination and cooperation in combating corruption, and that all proposals and ideas will be implemented and may cause adoption of effective laws and regulations.

RUSSIA IN THE INTERNATIONAL AML/CFT SYSTEM

HEADS OF FINANCIAL INTELLIGENCE UNITS OF THE CIS MEMBER STATES MET IN DUSHANBE

New work streams were set out during a meeting of the Council of Heads of Financial Intelligence Units of the CIS Member States

Irina V. Ivanova,
Chief Editor

A regular meeting of the Council of Heads of Financial Intelligence Units of the CIS Member States, chaired by Rosfinmonitoring Director Yu. A. Chikhanchin was held in Dushanbe (Tajikistan) on November 11, 2014.

The meeting was attended by delegations of financial intelligence units of states parties to the Agreement on the establishment of the CHFIU: Armenia, Belarus, Kazakhstan, Kyrgyzstan, Russia and Tajikistan.

A list of invited officials included: Deputy Head of the Anti-Terrorist Center of the CIS V.V. Soloviev, Executive Secretary of the Eurasian Group on Combating Money Laundering and Financing of Terrorism (EAG) B.V. Toropov and General Director of the International Training and Methodology Center for Financial Monitoring O.A. Ivanov.

That meeting of the Council of Heads of Financial Intelligence Units of the CIS was the first after the Belarus council of heads of state of the CIS in October, which approved amendments to the Agreement on the CHFIU.

The agenda of the meeting of heads of financial intelligence units in Dushanbe consisted of 14 items, among them: the FIUs Cooperation Framework, the 2015-2016 Activity Plan, the CIS FIUs Information Sharing Strategy. All these documents were approved by the Council. Representatives of Belarus and Russia also presented reports on the assessment of risks and threats related to combating money laundering and terrorist financing, as well as on the development of risk management procedures. In addition, participants' special attention was devoted to the topic on the search for and return of criminal assets in the CIS.

Rosfinmonitoring representative shared best practices in combating money laundering derived from drug trafficking and its precursors.

According to Russian FIU information trafficking of Afgan opiates passes through the CIS member states. The annual volume of Afgan market – biggest opium poppy producer for production of 90% heroin in the world – is about 65 billion USD. For example common financial assets of Afgan private and public banks (there are 17 banks at all) is about 4,7 – 4,9 billion USD. IMF shows that gold and currency reserves in the country are about 6,2 – 6,3 billion.

Legalization of drug trafficking proceeds is a global threat for global economic and political security now.

To compare with the first 6 months of 2013 the number of drug crimes has increased in all the CIS member states, apart from Armenia and Kazakhstan.

Now it`s necessary to solve a problem of prevention transnational criminal organizations activities out of any borders. That is the reason effective counteraction should be "out of borders" too. For this aim financial intelligence units have to develop their interaction, more actively facilitate coordination with law enforcement authorities within countries, pursue counter drug business and drug-related funds set of measures. All of this require coordination of efforts and improvement activity effectiveness.

Following the presentation were announced main directions for FIUs cooperation in this field. In order to reduce the risk of penetration of transnational drug trafficking groups' dirty money into the CIS financial systems and its subsequent laundering, it was decided that additional measures designed to facilitate the rapid exchange of the relevant data between FIUs should be developed.

The number of drug crimes

Country	the first half of 2013	the first half of 2014	% to the total amount of the registered crimes in the firs half of 2014
Azerbaijan	1 549	1 822	15
Armenia	593	537	6
Belarus	2 182	3 618	8
Kazakhstan	2 032	1 884	1
Kyrgyzstan	924	936	7
Moldova	503	601	3
Russia	114 812	123 987	11
Tajikistan	519	615	6
Ukraine	18 399	...	-

One more result of the meeting is creating of the next year`s CIS Anti-Terrorism/Extremism Financing Activity Plan. It assumes realization of joint checks. There 5 main directions of such events: contractors (persons who took part / participate now in bilateral conflicts it states with a high terrorist activity), migrants (persons who are involved in illegal migration within the CIS), couriers (persons systematically transfer cash through state borders), non-profit organizations (identification of transactions related to terrorism/extremism financing activity) and list of organizations and individuals known to be involved in extremist and terrorist activity – there is a perspective project of creating general list for all CIS member states.

This document was approved by the Council.

Following the meeting, participants took a number of decisions on key issues, including a decision to establish a working group on AML/CFT risks and threats assessment.

The meeting of the Council of Heads of Financial Intelligence Units of the Commonwealth of Independent States was held in a spirit of mutual understanding, trust and constructive dialogue.

The joint efforts of the CIS financial intelligence units help to ensure the use of an integrated approach in solving problems of stability and security strengthening, modernization of the organizational and legal systems as well as the introduction of cooperation instruments appropriate to modern requirements.

The next meeting of the Council will be held in May 2015 in Bishkek (Kyrgyzstan).

EAG CAN RIGHTFULLY BE CONSIDERED TODAY THE BEST FATF-STYLE REGIONAL BODY

The 21st EAG Plenary meeting, which first day was devoted to the 10th anniversary of the Eurasian Group on Combating Money Laundering and Financing of Terrorism (EAG), began in Dushanbe (Tajikistan) on November 12, 2014

Irina V. Ivanova,
Chief Editor

The history of the EAG dates back to October 6, 2004, when in Moscow the attending parties signed two documents that laid the foundation of the organization:

- The Declaration on the establishment of the Eurasian Group on Combating Money Laundering and Financing of Terrorism;
- Terms of Reference of the EAG.

In 2011, the EAG was granted the status of an international intergovernmental organization.

During his speech, Yu. A. Chikhanchin, head of the Russian delegation, chairman of the EAG in 2012-2013 and director of Rosfinmonitoring, reminded participants of the organization's long path of

Yury Chikhanchin hold the EAG jubilee medal

development: today all EAG member states have well-functioning national anti-money laundering systems, legal frameworks that support them and financial intelligence agencies:

«Without a doubt we have come a long way and the organization that Russia has delivered into the hands of our Indian colleagues can rightfully be considered today the best FATF-style regional body in the world. Thank you for believing in Russia and for following it. It shouldn't have been any other way, I suppose, given that at its helm was the man credited for creating the Russian Financial Intelligence Service – Viktor Zubkov.»

The head of the Russian Financial Intelligence Service recalled how likeminded people from Belarus, Kazakhstan, Kyrgyzstan and China became the backbone of the EAG:

«The main result of our work is our unity and the coming together of all the members of the Group we see here today… We have learned to listen to each other and help each other, as evidenced by Turkmenistan, Kyrgyzstan, Tajikistan's exit from the FATF's grey list. Now we can say that the EAG is beginning a new round of evaluations with a clean slate.»

Summing up the success of the EAG, Mr. Je-Yoon Shin, vice-president of the FATF and head of the Financial Intelligence Unit of the Republic of Korea, said: the EAG currently consists of 9 members, 16 observers and 17 regional and international organizations:

«Money laundering and terrorist financing represent today global problems that require global solutions. As financial markets become increasingly globalized, the role of the EAG and FATF in the fight with these problems increases. Criminals always target the weakest link in the financial system. That's why we need to act together. The international standards that are embodied in the FATF recommendations should form the basis of every country's fight against money laundering and terrorist financing.»

Representative of the FATF Timothy Goodrick reminded participants that new methodology puts at the forefront the task of increasing the effectiveness of national AML/CFT systems and using a risk-based approach:

«Although the new methodology poses new challenges for the mutual evaluations, by coordinating their efforts the FATF and FSRBs will be able to overcome them. We are as strong as strong our weakest link.»

Words about the EAG and the EAG Secretariat were spoken by representatives of Belarus, India, Kazakhstan, China, Kyrgyzstan, Turkmenistan Uzbekistan and some of its partner FATF-style regional bodies: APG, MENAFATF and MONEYVAL. The attending observers from the OSCE, World Bank, Afghanistan, Montenegro, Turkey and other countries also noted the importance of the work carried out by the EAG. In particular, the CSTO noted the importance of joint practical measures implemented in the framework of the regional anti-drug operation «Channel», while the U.S. congratulated Tajikistan and Kyrgyzstan on removing from the FATF's grey list.

A representative of the UNODC urged to focus on effective enforcement, as an assessment

carried out by this organization shows that only a small proportion of criminal proceeds end up being seized.

«The EAG is actively involved in the FATF's work and acts as a conductor of the principles and procedures of this organization in the region. And we, while showing consolidated political will, reaffirm our commitment to these principles and procedures. We also reaffirm our commitment to the EAG's goals and the principles of the United Nations in the field of peace and security.»

Anniversary medals «10 Years of the EAG» were awarded to the representatives of Belarus, India, Kazakhstan, China, Kyrgyzstan, Russia, Tajikistan, Turkmenistan, Uzbekistan, Ukraine and other countries.

Dzhuma Davlatov- Assistant to President of Tajikistan hold the EAG jubilee medal

PLENARY MEETING THAT MARKED THE TEN YEARS HISTORY OF THE EURASIAN GROUP

The 21st Plenary Meeting of the Eurasian Group on Combating Money Laundering and Financing of Terrorism (EAG)

Irina V. Ivanova,
Editor-in-Chief

Konstantin V. Litvinov,
Deputy Editor-in-Chief

In his welcome address, Mr. Bisengali Tadzhiyakov, the EAG Deputy Chairman, pointed out:

"Efficiency of the performed work is proven by the fact that all EAG member states have fully operational national AML/CFT systems supported by the adequate legal and institutional framework. The sectoral and international cooperation enjoys steady development, and the EAG is successfully completing the first round and will soon start the second round of mutual evaluations... At present, none of the EAG member states is included in the FATF lists, which is the definite success indicating that the EAG is on the right track".

At the closed session of the Plenary, participants were informed about replacement of the current head of the Group: Mr. Ajay Tyagi, the Republic of India, was elected as the EAG Chairman until the completion of Dr. K.P. Krishnan's Action Plan for 2014-2015. The Indian delegation informed that Dr. K.P. Krishnan was appointed to other office in the Indian Government and Mr. Ajay Tyagi became his successor. In this context, the Indian Government nominated him as a new Chairman of the EAG. The Indian delegation thanked all EAG member countries for unanimous support of its nominee. In his turn, Mr. Bisengali Tadzhiyakov, who chaired the Plenary Meeting, on behalf of all delegates expressed gratitude to Dr. K.P. Krishnan for the performed work.

Another important issue on the agenda was replacement of the EAG Executive Secretary: Mr. Boris V. Toropov, who held this office since

2011, resigned, and Mr. Vladimir P. Nechaev, who served as the FATF President in 2103-2014 and headed MONEYVAL in 2010-2013, was appointed to this vacant position.

Besides that, the issue of granting the observer status to the Islamic Republic of Iran was raised and considered by the EAG Plenary: Iran formally requested the Group to consider possibility of granting it the observer status and providing technical assistance. The Plenary attendees with a great interest listened to the presentation made by Mr. Meisam Nasiri Ahmadabadi, Director General of the FIU in the I.R. of Iran. Following the discussion, it was decided to examine possible observer status of Iran in line with Article 8 of the Agreement on the EAG and put this issue on the table again at the EAG 22nd Plenary.

The Plenary was briefed on the review of Kyrgyzstan and Tajikistan under the ICRG process. The delegates of the EAG member states congratulated their colleagues with removal from the FATF follow-up process.

The delegations of Belarus, India, Kazakhstan, China and Russia provided information on national AML/CFT legislation amendments. After that, the Plenary heard the reports on progress made by the Kyrgyz Republic, Turkmenistan and the Republic of Uzbekistan.

Besides that, the FATF representatives shared the experience gained in course of mutual evaluation of Spain and Norway.

Mr. Pavel V. Livadny, State Secretary and Deputy Director of Rosfinmonitoring, pointed out that the EAG 21st Plenary marked the ten years history of establishment of this Group which, throughout these years, has gained an international reputation and has become one of best FATF Style Regional Bodies:

"The FATF has started the next round of mutual evaluations of the national AML/CFT systems, and it sets the EAG the similar objectives. The new Assessment Methodology is mainly focused not on assessment of the legal and institutional framework, but on effectiveness of the AML/CFT system in fighting against economic crime. What is the value and amount of confiscated assets generated from crime, and what are the outcomes of combating the financing of terrorism, extremism and other ant-social activities? Currently, the FATF applies very strict criteria and approaches to conducting assessments. Just as an example, Norway, being one of the FATF founders with the developed financial system, economy and legislation, received relatively poor ratings in course of the new round of evaluations. In this context, it is clear that our countries have to take the lessons learned into account".

The 22nd Plenary meeting will be held next May in Tashkent, the Republic of Uzbekistan.

Timothy Goodrick, policy analyst at FATF:

First of all I want to say that the Eurasian Group is currently celebrating its 10th anniversary. It has come a long way during that time, from the moment when there was no FSRB in the region to the emergence of a full-scale regional group that rightfully occupies its place in the international AML/CFT system.

With regard to the 21st EAG Plenary meeting, I'd like to mention at the significant progress achieved by Kyrgyzstan and Tajikistan in terms of bringing its AML/CFT legislation in line with international requirements, as evidenced by their removal from the ICRG process, the fact highlighted at the current EAG Plenary.

Zhang Yang, section chief the AML Bureau, People's Bank of China:

I think the most important issues of the plenary week were the approval of the procedure for the second round of mutual evaluations and the adoption of certain internal documents relating to changes in national AML/CFT legislations of EAG member states. Equally important were the re-election of the EAG chairman and the adoption of the next year's action plan adoption.

Pankaj Kumar Mishra, assistant secretary of deputy minister, Ministry of Finance, Government of India:

The plenary week was dedicated to the formation of the EAG, which, naturally, was an important milestone. We discussed many issues, including changes connected with the implementation of the FATF standards, experience sharing among EAG member states and other issues that are intended to help all members and observers of the Eurasian Group.

All working groups have done a very good job, particularly - the Working Group on Supervision, which generates today considerably more interest among the participants than in the previous years. Separately, I would like to mention the contribution to the development of the EAG made by the EAG Secretariat. I think if we continue to work with the same vigor, as the same cohesive and strong team, the results of our work will have a major impact on the next round of mutual evaluations.

Vladimir P. Nechaev (Russia), EAG Executive Secretary since January 2015:

«I'd like to note that the EAG has approached its 10th anniversary with a very impressive result: it has become the first FATF-style regional body with not a single member under FATF monitoring process, an achievement that underscores the great progress made by our countries in strengthening their anti-money laundering systems.

The Plenary made a decision to grant observer status to the CIS Anti-Terrorist Center that shows both EAG prestige and its desire to coordinate the efforts of regional organizations towards the common goal of combating money laundering and terrorist financing.

I think the approval of the Procedures for conducting the second round of mutual evaluations and the EAG's 2015 Action Plan is very important because it represents an increased emphasis on practical steps to prepare and conduct a new round of mutual evaluations based on the new FATF standards.»

Section on Counteraction of Financing Drug Business and Crime (WGCF)

The Working group on counteraction of financing drug business, crime and terrorism (WGCF) of the Eurasian Group on Combating Money Laundering and Financing of Terrorism (EAG) was created in May 2012.

EAG member states and some observers arranged the WGCF as a platform for mounting joint efforts to uncover the financial infrastructure of the drug trafficking.

The Group devotes particular attention to the joint events focused on detecting and suppressing illegal

activities of individuals and legal entities involved in the laundering of money and assets acquired with drug proceeds. Herewith the main efforts are concentrated on the detection of transnational criminal groups engaged in the legalization of proceeds derived from drug trafficking.

Based on the results of the WGCF work in 2013, the 18th EAG Plenary in Minsk adopted the Guidelines for participation of the EAG member states and observers in the CSTO's regional anti-drug operation «Channel», containing a mechanism for the participation of Financial Intelligence Units (FIUs) of the EAG in the operation «Channel» and recommendations for the use of concerted efforts to combat the financial component of the drug business. The Guidelines were developed based on Rosfinmonitoring's experience of participating in the operation «Channel» and are currently being effectively applied by the FIUs of EAG member states.

Currently, the Group's efforts are directed at uncovering the financial component of the Afghan drug business. This work is being carried out at the international and national levels, in cooperation with law enforcement agencies of EAG member states and observers.

For the first time was created a common bank of criteria of suspicious financial transactions allegedly linked to drug trafficking, containing a total of 31 criteria. The work to expend the bank of criteria will be continued in the future.

A list of other activities carried out by the Group includes efforts to map the geography of financial flows, identify the countries involved and compile a list of credit institutions linked to the financial component of the drug business. The Group is conducting researches of contactless drug trafficking schemes based on electronic payment systems made via landline and mobile communication channels. The Group is gradually gaining experience in identifying drug trafficking offences through the analysis of financial transactions. The work carried out in this area allowed, for example, the Financial Intelligence Units of Russia, Kyrgyzstan, Kazakhstan, Tajikistan and national law enforcement agencies of these countries to identify and suppress in 2013 a drug trafficking channel used for delivery of drugs from Afghanistan to Russia.

Some joint financial investigations are being conducted at the moment. The Group's efforts aimed at uncovering the financial component of the drug business helped reveal the involvement of intermediary offshore companies in schemes to distribute the proceeds credited to their accounts and make payments on behalf of third parties for goods and services provided under foreign trade contracts.

The 18th EAG Plenary meeting (May 2013, Minsk) approved launching an international study titled «The use of companies registered in offshore jurisdictions for redistribution and laundering of criminal proceeds», which aims to develop country-specific measures necessary for the effective detection of such companies.

During the 20th and 21st EAG Plenary meetings (June 2014, Moscow; November 2014, Dushanbe), the Russian Federation proposed a new approach to the detection of suspicious entities allegedly linked to the redistribution and laundering of criminal proceeds through the accounts of offshore companies.

In addition, the Group compiled a list of countries and territories classified under the laws of EAG member states as offshore jurisdictions, as well as identified countries that, although not included in the official list of offshore jurisdictions, may, in the opinion of EAG member states, be used for money laundering.

This work has allowed the Group to identify jurisdictions, both offshore and non-offshore, that may be of interest to the Group in some areas of its activities.

As a result of the current research, the Group expects to identify offshore companies suspected of being used for money laundering, together with credit institutions involved in dubious financial schemes with Russian companies and banks of EAG member states and observers.

The practical results of the Group's work are also highly valued by EAG observers. The regular WGCF meeting in November 2014, in Dushanbe was attended by all EAG member states and the following observers: UNODC, Afghanistan, Turkey and the United States.

The Group also Discussed and approved the WGCF's 2015 Action Plan.

BEST EXAMPLES OF COOPERATION BETWEEN GOVERNMENT AGENCIES IN CONDUCTING FINANCIAL INVESTIGATIONS

During the 21st EAG Plenary, Rosfinmonitoring made a presentation of a financial investigation conducted by its Volga Federal District Inter-regional Department and submitted as an entry to the Contest for the best financial investigation. The investigation was carried out not only in close collaboration with law enforcement agencies, but also in partnership with the Federal Tax Service of Russia, the Federal Service for State Registration, Cadastre and Cartography (Rosreestr) as well as multiple reporting entities.

In this issue of the Financial Security journal, we offer our readers to have a look at the Russian presentation, which, together with the Chinese entry, was voted winner of the contest. The presentation was delivered by Konstantin I. Gobrusenko, deputy head of Rosfinmonitoring's Anti-Money Laundering Department.

K.Gobrusenko and B. Tadzhiyakov

The financial investigation in question was triggered by an inquiry made by the Ministry of Interior of the Republic of Tatarstan in connection with a criminal case against Mr. "C" and several of his associates involving alleged fraud and theft from private individuals of securities issued by one of Russia's largest energy companies.

It should be noted that it has become a standard practice in Russia for Rosfinmonitoring employees to hold working meetings with police detectives and investigators to discuss high profile criminal cases and cases against organized criminal groups.

Following a working meeting with law enforcement officials of the Republic of Tatarstan, it became clear that Mr. "C" and three of his accomplices, while using the services of a private notary, committed large-scale fraud and breach of trust in 2006-2009 in order to take possession of other persons' property (securities issued by Russia's largest energy company).

A question arose: what are the perpetrators going to do with these securities? After discussing the details of the investigation and the upcoming operational and search activities at several working meetings, investigators came to an opinion that the perpetrators would try to sell them.

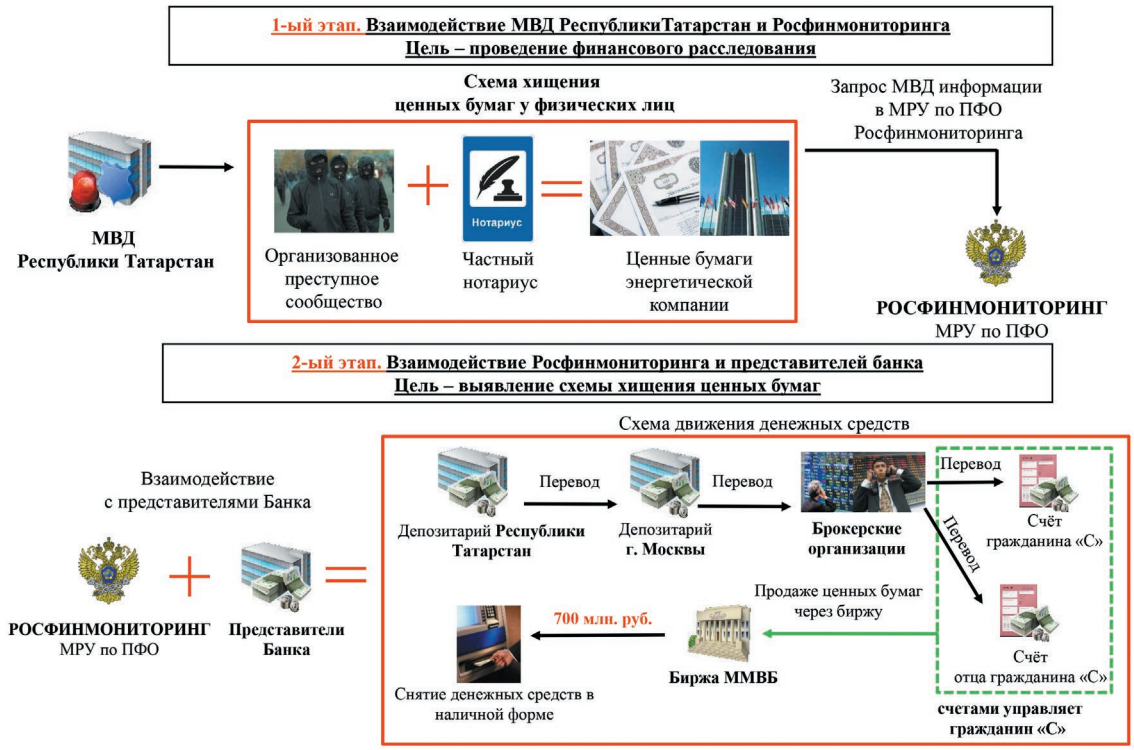
Using the information available, an analyst tried to predict how the fraudsters may dispose of the securities and where they may invest the criminal proceeds. First, he suggested that they might have concluded a custodial agreement with a financial institution – it turned out to be a good supposition. After analyzing data submitted by reporting entities, the analyst ascertained that the fraudsters had placed the securities with one of Tatarstan's custodial institutions.

By acting in close collaboration with Tatarstan's law enforcement officials, Rosfinmonitoring established contact with this institution and obtained details of all custodial transactions conducted by the fraudsters, as well as uncovered the scheme for the future movement of stolen securities. After being granted the right to dispose of the securities, Mr. "C" decided to transfer them to a custodial institution in Moscow to cover his tracks.

Following this development, investigators requested Rosfinmonitoring to establish contact with this Moscow institution, which revealed that Mr. "C" had opened depositary accounts with it for himself and his elderly father, both of which he controlled.

All depositary account transactions with securities are recorded by the bank as off-balance sheet items (*values other than bank's assets*).

General scheme of cooperation within financial investigation



The bank's replies to Rosfinmonitoring's inquiries helped reveal that Mr. "C" had entered into agreements with three brokerage firms to help him dispose of the securities. At the request of their customer – Mr. "C" – these brokerage firms placed orders to sell securities on the Moscow Interbank Currency Exchange.

When trading under the DVP (delivery vs. payment) settlement procedure, every movement of money and securities takes place within the exchange and only with the use of each broker's unique ID. Furthermore, the broker ties his customers' depositary accounts participating in the trade to his own accounts to which funds are credited at the end of the trading session.

All this allowed the investigators to establish the amount received by Mr. "C" from the sale of the securities – approx. 700 million rubles.

The results of the investigation were then discussed at a working meeting with the staff of the Ministry of Interior of the Republic of Tatarstan. A proposed action plan involved the initiation of coordinated measures designed to identify and keep track of all expenditures and investments made by Mr. "C" and his associates using the criminal proceeds.

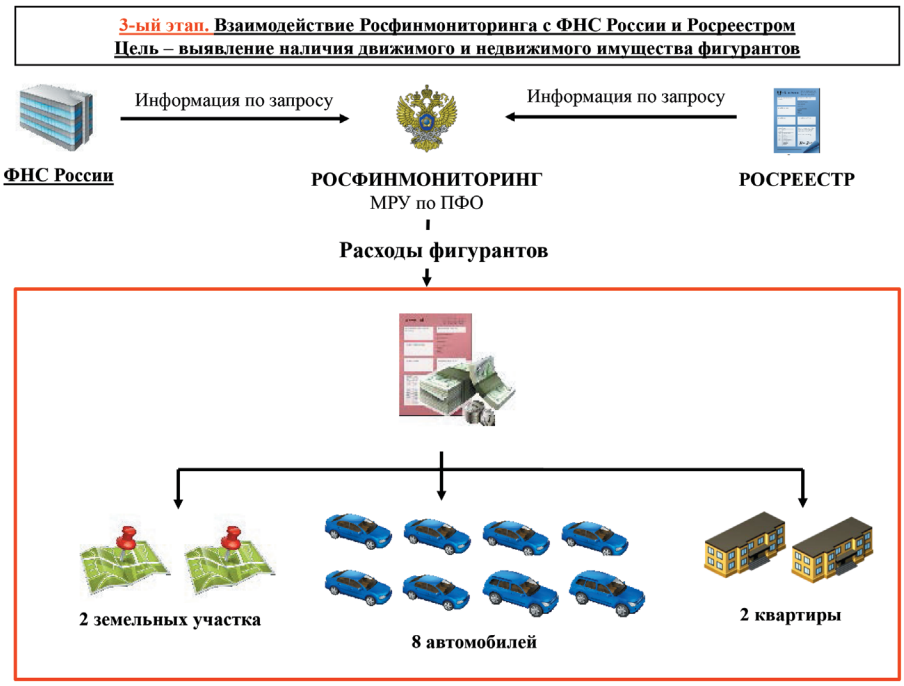
To this end, Rosfinmonitoring worked closely with Rosreestr to reveal the purchase by the fraudsters of two plots of land and two apartments.

Concurrently, Rosfinmonitoring established cooperation with the Federal Tax Service of Russia, which showed that the defendants' expenditures exceeded their declared income and that they, in addition to the two land plots and two apartments, purchased also eight cars.

Due to the fact that the above defendants' actions fall within the definition of money laundering, we decided to submit the findings of the financial investigation to the Ministry of Interior of the Republic of Tatarstan, which involved the disclosure of banking secrecy. Based on materials submitted by Rosfinmonitoring and their subsequent discussion at a separate working meeting, the Interior Ministry of the Republic of Tatarstan requested the necessary documents from the executive authorities and organizations concerned, which were then successfully used in criminal proceedings.

The evidence uncovered during the investigation was used to open on March 14, 2011 three money laundering cases, subsequently merged into a single criminal case involving the following predicate offenses: «Fraud committed by a person using his official position or by an organized group or on a large scale», «Extortion committed by an organized group», and «Abuse of office by a private notary or private auditor with the goal of gaining benefits and advantages for themselves or others».

General scheme of cooperation within financial investigation



On November 12, 2013, the Vakhitovsky district court of the city of Kazan found Mr. "C" guilty of, among others, money laundering and sentenced him to eight years in prison. Mr. "C"'s accomplices were sentenced to 6 and 4 years in prison respectively.

***

Issues of interagency cooperation are given priority in Russia. On July 31, 2012, Russian President Vladimir Putin signed a decree «On the Interdepartmental Working Group on Combating Illegal Financial Transactions» (IWG), headed by the assistant to the President of the Russian Federation E. M. Shkolov. The signing of this degree underscores the priority given to this area of activity in the government's public policy. The IWG is a coordinating body established to ensure effective cooperation between federal executive authorities, other public bodies and the Central Bank of the Russian Federation (Bank of Russia) in preventing, detecting and suppressing illegal financial transactions, as well as in combating illicit capital flight. In addition, regional branches of the IWG have since been established under special representatives of the President of Russia in different regions.

Although the created interaction system has already shown its effectiveness, we believe it can still be improved, including by borrowing the best experience and practices of our foreign partners.

INTERNATIONAL BLOCK

JOIN OUR EFFORTS TO CONDUCT NEW ASSESSMENTS

Training workshop for EAG assessors was held in New Delhi (India), on October 6-10, 2014 in the framework of preparations for the second round of EAG mutual evaluations

The event was oriented at training of representatives of EAG member states' delegations who will be engaged as assessors and analysts in the second round of EAG mutual evaluations.

The workshop was opened by the EAG Chairman Dr. K.P. Krishnan (India), Deputy Director of Rosfinmonitoring V.I. Glotov (Russia) and Executive Secretary of EAG B.V. Toropov (Russia).

The EAG assessors training coincided with the tenth anniversary of signing on October 6, 2004 of the EAG Declaration and the Terms of Reference. That fact was mentioned by speakers during opening of the event that became a traditional example of horizontal cooperation within FATF family.

Besides administrators of the EAG Secretariat, competent employees of the FATF and the APG secretariats were invited to the workshop.

Attending as trainees were representatives of all EAG member states, and some APG member states, employees of the Secretariat of the Interregional Group on Anti-Money Laundering in the Western Africa (GIABA).

Trainees attended a course of lectures on methodology and procedures of holding of mutual evaluations based on the ad hoc package of training materials that had been developed by the FATF for the event. At the end of the training, participants held a practical class in mutual evaluation of the national AML/CFT system of "X state".

We should also emphasize a high level of workshop organization made by India and participants' wish to hold such events in future in order to improve experts' knowledge and skills.

***

On October 11, 2014, the workshop on national risk assessment was held in New Delhi (India).

During the event, the Russian delegation presented the National Center of Risk Assessment established on the basis of Rosfinmonitoring.

The workshop was attended by representatives of relevant institutions of the Republic of India as well as delegates of Belarus, Kazakhstan, Tajikistan, Uzbekistan and the EAG Secretariat.

The participants were introduced methods of information gathering and processing as well as technologies of received data analysis.

Issues of implementation of available technological solutions within the Eurasian Group were also discussed during the event.

A PRIMARY GOAL IS COMBATING TERRORIST FINANCING

A Russian government delegation, headed by Rosfinmonitoring Deputy Director V. I. Glotov, took part in the expert and working group meetings and 26th Plenary session of the Financial Action Task Force (FATF), held in Paris on October 19-24, 2014

Irina V. Ivanova,
Chief Editor

It was the first session held under the chairmanship of Australia (R. Wilkins), after the termination of the Russian presidency of V. P. Nechaev on July 1, 2014.

Among the key issues discussed at the meeting were:

- review of the first mutual evaluation reports prepared as part of the new, fourth round of mutual evaluations (Spain and Norway);
- updating the FATF's black and grey lists and revision of the procedures for their formation in light of the newly adopted mutual evaluation guidelines;
- more effective use of the FATF tools in the fight against terrorist financing in the context of the growing terrorist threat;
- admission of new members to the FATF;
- banks' reluctance to deal with high-risk customers (de-risking).

Following the review of the first mutual evaluation reports of the fourth round, Spain was put on the regular monitoring process, while Norway on the enhanced monitoring process due to some serious shortcomings with regard to both technical compliance and effectiveness of the national AML/CFT system.

After hearing the above reports, delegations shared their views about the difficulties and problems emerged in the course of the first country evaluations conducted in accordance with the 2013 FATF Methodology. It became apparent that it was necessary to amend the Fourth Round Guidelines, adopted in February of this year. A list of proposed amendments includes the extension of the timeframe allowed for each evaluation stage and redistribution of the available resources.

The work to review the criteria for compiling the black and grey lists, which started in June 2013, was resumed, with participants discussing the possibility of using performance metrics as the main criteria for

placing jurisdictions on this type of monitoring. At this stage, most delegations take the view that the adoption of such approach prior to obtaining the necessary practical experience and the full review of the new round of mutual evaluation mechanism is premature.

The study aimed at ensuring effective supervision and law enforcement activities is gaining momentum. The reference points of the future document have already been agreed, while the best practices expected to be added soon. In addition, participants decided to intensify the study of the use of virtual currencies for ML/FT.

A discussion of progress made in implementing the FATF Secretariat-approved action plans to remedy the strategic shortcomings in the national AML/CFT systems revealed that not a single blacklisted jurisdiction (Algeria, Indonesia, Iran, North Korea, Myanmar and Ecuador) has managed to exist the black list since June.

As for Indonesia and Ecuador, the next few months are going to be absolutely crucial for them, given that under the existing procedures. If they fail to show significant progress by the start of the next plenary (February 2015), the FATF may decide to move them to the toughest part of the list featuring North Korea and Iran, which are subject to the so-called countermeasures.

North Korea, on the other hand, is moving in the right direction: in July it joined the Asia-Pacific Group (an FSRB) as an observer, which speaks of Pyongyang's willingness to establish a constructive dialogue with the FATF community and eventually exit the black list.

With regard to Iran, the situation is unchanged: the main problem – terrorist financing – is still not adequately criminalized.

The plenary took a long-awaited decision to delist Turkey, which was recently visited by a FATF monitoring mission that saw at first hand that most of the problems with its national AML/CFT system had been addressed. Among other countries exiting the monitoring process are Cuba and Tajikistan, meaning that the Eurasian Group is currently the only FATF-style regional body with not a single member in the black or grey list.

As part of the final stages of the third round of mutual evaluations, the FATF continued its work with the member jurisdictions placed under enhanced monitoring process and still lacking enough progress to warrant delisting, among them are Brazil, Iceland, USA, South Africa and Japan. And while the United States and South Africa have achieved at least some progress, the situation with the rest remains pretty bad. The FATF plans to send to these countries high-level missions next year to carry out the necessary outreach activities.

The plenary devoted priority attention to the effectiveness of the fight against terrorist financing in connection with the escalation of terrorist activity in the world, with the CFT issue dominating not only the agenda of the meetings specifically dedicated to this topic, but also the discussions of country-specific issues.

Particularly meaningful was the discussion of the methods to combat the financing of the Islamic State of Iraq and the Levant (ISIL). Given the threat it poses, it was decided that this issue should be discussed by the FATF's Risks, Trends and Methods Working Group, with a report to be submitted to the next plenary meeting (February 2015). This project will be devoted to the study of the ISIL funding sources as well as its financing channels and mechanisms.

Following an exchange of ideas, the FATF President issued a public statement urging all countries to strictly comply with the FATF Recommendations with the view to denying ISIL access to the national financial systems. The document contains references to UN Security Council Resolutions 2170 and 2178 as well as to the specific FATF Recommendations (5, 6, 8, 10, 13, 14, 16, 32, 37, 39 and 40). It also notes that the FATF will continue to assess ML and FT risks linked to ISIL, including by examining its income sources.

The next Plenary meeting will be held in Paris again, in February 2015.

COUNTRY ANTI-MONEY LAUNDERING INDEX OF THE BASEL MANAGEMENT INSTITUTE

In August 2014, the Basel Management Institute presented its third annual anti-money laundering Index (AML Index)[1], which is calculated using the Institute's proprietary method in cooperation with the International Centre for Asset Recovery

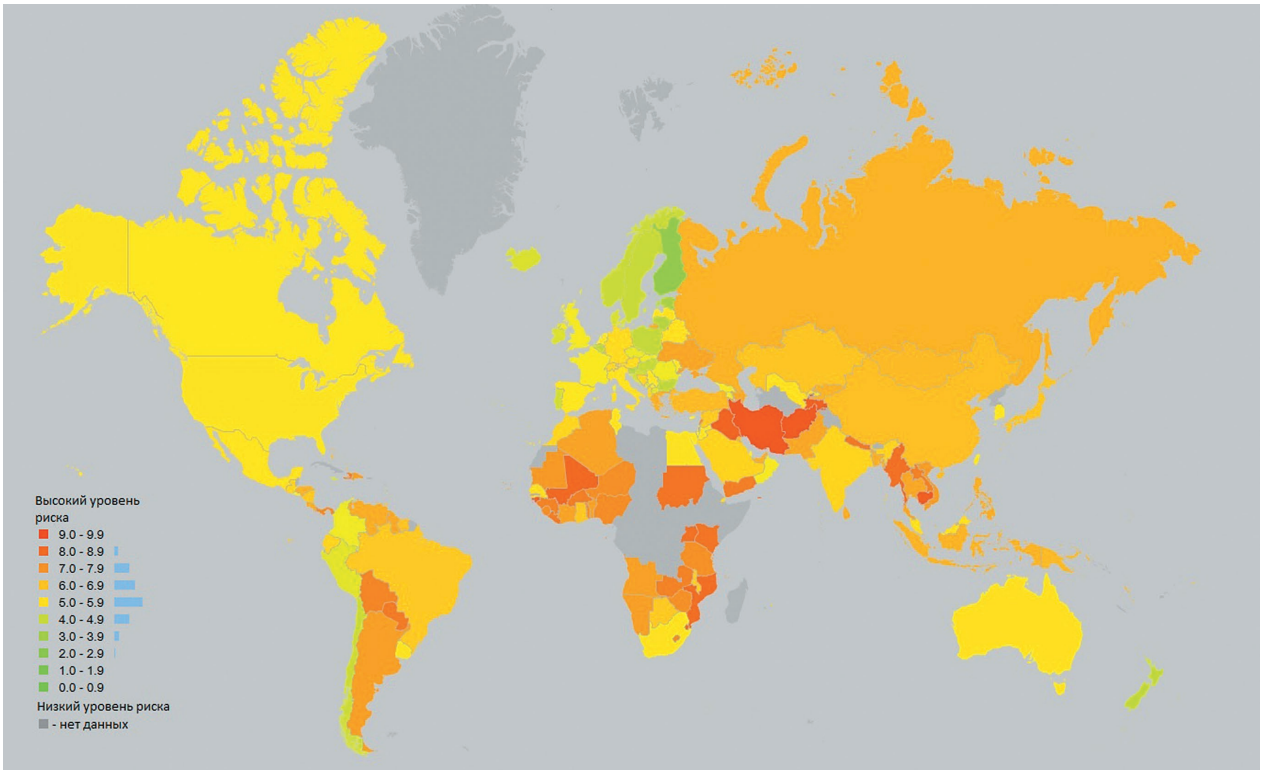
Nikita A. Bobryshev,
ITMCFM Project Manager

The Basel AML Index is a ranking assessing country risk regarding money laundering and terrorism financing (AML/CFT). It focuses on efficiency of implementation of AML/CFT measures as part of a specific state's system, with calculation comprising various related factors such as public and financial sectors transparency as well as judicial strength, etc.

The first research aimed at calculation of the AML/CFT index was held in April 2012, and until now the Basel AML index has been the only indicator to analyze country risks in this sphere through application of the research approach estimated by an independent non-profit organization. 2014 Index covers 162 countries with risk level ranging from 0 (low risk) to 10 (high risk) and reflects final ML/FT rating of a country. Today, neither uniform method to determine whether the country is under high risk nor clear definition of such situation exists. To this end, employees of the Basel Institute carried out an extensive research, following which the method for calculation of the final AML index was based on 14 external indicators to reflect various aspects of AML/CFT system functioning. All indicators may be divided into the following groups – corruption risks, political and legal risks, AML/CFT risks, transparency of financial sector, transparency and financial responsibility of the public sector.

FATF mutual evaluation reports are the main source of information used in index estimation (contribution to final index value of about 65%). It stands to mention that existence of developed institutional and legal base does not imply effective implementation thereof, so FATF conclusion may be not fully indicative of actual AML/CFT situation in a particular country. Such discrepancies may be eliminated as new recommendations and methods are introduced and the new round of mutual evaluations with emphasis placed on efficiency issues progresses.

[1] http://index.baselgovernance.org/index/Index.htm



In 2014, heading the list were Finland and Estonia – the only countries recognized by the index developers as zero-risk in terms of AML/CFT (index value lower than the limit of 3.3 points). According to calculation method, these states are distinguished by strong and efficient AML/CFT system, high level of financial and public transparency, and low corruption. Recognized as the most troubled countries were Iran, Afghanistan and Cambodia. It stands to mention that the Basel Index underlines the risks and vulnerability of the existing AML/CFT system on the whole rather than assessing quantitative characteristics of illegal financial transactions.

The Dominican Republic, Croatia, Macedonia and Saint Lucia demonstrated the best improvements against the previous year. These states mitigated their risks significantly and managed to improve the level of technical compliance with FATF standards, which was recorded in respective reports. The most significant negative changes concerned Brazil, the Republic of Cote d'Ivoire, Panama and Saudi Arabia. Vulnerabilities of tax legislation – in particular, tax secrecy – affected the negative rating of Brazil and Saudi Arabia. Low rating of other states is associated with great number of deficiencies specified in the reports of FATF and respective FATF-Style Regional Bodies.

As for the members of the Organization for Economic Cooperation and Development (OECD), Austria, Germany, Greece, Luxembourg, Japan, Switzerland and Turkey demonstrated negative trends. Despite certain improvements in AML/CFT sector as set out in FATF reports, these states may still be used for illegal purposes. During the last reporting year, Germany and Switzerland demonstrated strengthening of anti-money laundering mechanisms, efficiency of legal and political institutes as well as active counter-corruption measures. Nevertheless, low level of financial transparency and vulnerability to financial flows associated with drug trade[2] have an adverse effect on estimated value of the index.

Best performance among EAG member states was demonstrated by Belarus and Uzbekistan who closely follow the USA and Canada in the Basel Index. Other members of the regional group remain in the middle of the list and demonstrate moderate level of AML/CFT risk. However, positive dynamic of the EAG representatives starting from the date of publication of their first reports deserves being mentioned.

[2] http://www.state.gov/j/inl/rls/nrcrpt/2014/vol2/index.htm

RUSSIA PRESENTED 3d FOLLOW-UP REPORT TO MONEYVAL

On September 16, 2014, Russian delegation headed by Rosfinmonitoring Director Yu.A. Chikhanchin successfully presented its third follow-up report to the Committee of Experts of the European Council on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL)

Irina V. Ivanova,
Chief Editor

On behalf of Russia, the meeting of the Council of Europe (Strasbourg, France) was attended by representatives of the Ministry of Internal Affairs, the General Prosecutor's Office, the Ministry of Foreign Affairs, the Central Bank, the Federal Customs Service, the Ministry of Telecom and Roskomnadzor.

Despite the foreign political factors, MONEYVAL confirmed its commitment to FATF standards in demonstration of objective unbiased approach to discussion of our report. Serious law making work aimed at bringing the Russian anti-money laundering legislation in line with international standards that was carried out over the recent years received positive assessment of the European Community.

For this purpose, the respective Federal Law № 134-FZ was passed and entered into force. It eliminated basic comments of FATF and MONEYVAL. From June 2012, in Russia:

- the concept of beneficial owner was introduced, obligations and requirements to its identification were established;
- the mechanism for blocking of funds and property appeared, financial institutions were bound to take measures associated with freezing on respective grounds;
- the size of a block of shares in a credit institution, acquisition of which requires consent of the Central Bank, was reduced from 20% to 10%;
- threshold value of laundered funds was eliminated;

- currency, tax and customs legislation offences were referred to predicate crimes.

When presenting the report, **the Head of the Department of International Relations of Rosfinmonitoring A.G. Petrenko** said:

"All recent law making in Russia is performed with regard to forthcoming assessment mission of FATF/MONEYVAL/EAG. In general, our country keeps working on implementation of recommendations of MONEYVAL experts, and this activity enjoys support of the highest level. Despite certain achievements on removing of the Russian Federation from FATF's monitoring process, development of the national anti-money laundering system continues.

Some federal laws were amended to prohibit previously convicted persons from holding senior positions in leasing companies and insurance organizations and to tighten the procedure for registration of legal entities in order to enhance transparency of the structure."

Main questions addressed to the delegation concerned the procedure of terrorist assets freezing, volumes of funds blocked in accordance with Resolution 1267 of the UN Security Council, and measures meant to secure transparency of beneficial ownership. The mechanism of application in Russia of FATF Recommendation 6 (concerning politically-exposed persons as revised in 2003) awoke great interest among participants.

The Russian Federation notified that the work was underway in establishment of legal mechanisms aimed at potential application of confiscation of money, value and other property acquired through crime as other criminal law measures.

Specifically, in his answers, representative of the Russian delegation particularized the issue of distant monitoring implemented in financial intelligence unit of Russia.

– As for the AML/CFT supervision of liable entities a distant compliance supervision mechanism has been recently introduced in Rosfinmonitoring. The idea behind this mechanism is to effectively apply supervision measures to liable entities (financial institutions and DNFBPs) distantly (saving time and resources) through the risk matrix comprised of risk factors.

To make it simple electronic registries for each type of financial institution or DNFBP has been established in the distant compliance supervision system (for leasing, real estate, securities, etc.).

All organizations of each particular registry undergo the so-called scoring or checking against internal and external (law enforcement and data from other authorities) risk-factors.

There are two major risk groups: AML/CFT noncompliance risks (that is when organization is registered within Rosfinmonitoring or Central Bank but does not file STRs or organization is not registered within supervisory body but conducts transactions, etc.). ML risks (that is when organization is involved in conducting suspicious transactions and perform suspicious behavior). The third group is TF risks, (that is the risk of not working with designated lists of terrorists, interaction with high risk territories etc.). For each group a comprehensive list of risk indicators has been established.

Each organization is checked against risk-factors and gradual (step by step) measures applying system is performed. If the scoring of a risk for a particular organization or groups of organizations is relatively low (for example registered but sending a low number of STRs due to some reasons) then special advisory letters are being issued by Rosfinmonitoring or Central Bank and sent to those organizations to eliminate defficiences as a first step of measures taking procedures. If the risk is high then a supervision mission may be arranged, in some cases jointly with law enforcement agencies, or license revoked or suspended.

All the checking and scoring is done automatically covering financial sectors on regular basis. And, as it was said, if a risk is relatively low or there are some technical deficiencies then letters of concern are being issued. Otherwise more serious steps are taken.

FATF member countries, EAG and FATF secretariats who attended country's session went all out in support of Russia. MONEYVAL secretariat put forward an initiative to remove from the agenda defense of the follow-up report until 2017.

Generally, in assessment of national anti-money laundering systems and their compliance with international standards, Europeans demonstrated a fundamentally new approach, with special attention paid to efficient implementation of legislation rather than general accomplishment thereof. MONEYVAL experts emphasized the importance of enhanced measures of economies decriminalization including such enhancement through considerable tightening of criminal law – increased responsibility for laundering and introduction of criminal liability of legal entities.

When discussing the outcome of the progress report presentation, the head of the Russian financial intelligence unit Yu.A. Chikhanchin said,

"We are content with the report presentation. MONEYVAL member states remained committed to standards elaborated by international community based on purely professional assessment of AML/CFT systems, beyond the influence of any political and ideological factors."

THE JOURNAL GUEST

PRESENTED CASE STUDIES MAY TELL ABOUT EFFICIENCY MORE THAN REAL STATISTICS

Interview with the Executive Secretary of MONEYVAL John Ringguth

John Ringguth

***FS:** Mister Ringguth, what issues discussed at the 45th MONEYVAL Plenary do you think deserve special attention?*

J.R.: Considering that combating the financing of terrorism is an important element of our mandate, the issue of the ISIL–the Islamic State of Iraq and the Levant–was raised in the first place. We held the meeting shortly after dreadful murders of the three hostages and observed a minute of silence in their honor. Then, we reminded the delegations that in August the UN Security Council Committee entered six persons associated with ISIL in the al-Qaida Sanctions List. Therefore, MONEYVAL requested their states and territories to confirm that all financial institutions and designated non-financial business or professions were aware of the new persons. It was suggested that MONEYVAL states and territories submit the Group any information concerning measures adopted to communicate data on such persons to private sector. In December, we will review the responses and – ignoring mutual evaluation reports – discuss how effective the list system is to all countries – whether they apply 1267 and 1373 Resolutions directly or using the mechanisms elaborated by the European Union. Delegations will be recommended bringing up problematic issues for discussion.

Second, in the course of preparations to the next round of evaluation, we will all know more about financing of proliferation. We received the presentation prepared by Dr. Jonathan Brewer of the Expert Group of the UN Security Council on 1929 Resolution (2010) dedicated to sanctions associated with financing of proliferation in Iran. Dr. Brewer defined the key moments including requirements of resolutions, role of the Sanctions Committee and the Expert Group as well as various types of possible sanctions. He emphasized the necessity of urgent inclusion of new persons on the national level. The latter consideration causes some similar problems, and countries still try to implement 1267 and 1373 Resolutions as regards urgent inclusion of persons in the lists.

We are approaching the end of the unique fourth round of mutual evaluations where efficiency was given particular emphasis. The 45th meeting passed the Estonian report on the fourth round within the framework of existing procedures. When discussing the report, we had a fair debate that gave rise to an interesting discussion concerning the level of evidentiary base needed for particular types of independent investigation of money laundering cases. Given successful investigation, these cases may definitely demonstrate efficiency of national systems in terms of ML criminalization.

***FS:** Queen Maxima attended the last MONEYVAL Plenary and spoke on the issue of financial inclusion. What is the reason for such careful attention to this issue?*

J.R.: Her Majesty's visit to the meeting was a great honor to all of us, since Her Majesty is a significant player in this issue. She reminded us that AML/CFT measures and financial inclusion policy were not mutually exclusive but complementary.

Promotion of wider official financial inclusion plays the key part in effective and integrated AML/CFT regime. Financial inclusion is an important issue to FATF and governments. National risk assessments receive increasingly greater consideration in some countries – especially, where extensive shadow economy is present. In many countries, involvement in financial system of greater numbers of people for the purposes of social development is a political priority. Financial inclusion features some AML/CFT advantages – the more we use the regulated sector, the less are the risks of money laundering and financing of terrorism via the shadow sector. We described the current situation with financial inclusion in MONEYVAL states and territories in our first report on this issue, which is published on our web-site. I recommend it to your audience.

***FS:** What are the prospects for development of this issue (financial inclusion) in the context of MONEYVAL activity?*

J.R.: This report will not be a single MONEYVAL event. Financial inclusion potentially affects the two spheres supporting operations of the Council of Europe – assistance in realization of human rights (in this case, apparently, the right to financial services); securing supremacy of law (through suppression of wider use of unofficial and illegal systems of bank and money transfers). As a body of the Council of Europe, MONEYVAL resolved that the issue required more attention. While social and political significance of financial inclusion is clear, actual influence of financial inclusion policy on AML/CFT remains less obvious.

MONEYVAL will hold similar researches once every two years in order to more accurately monitor development of financial inclusion in MONEYVAL states and territories during the period, and to analyze the effects it may have on AML/CFT in MONEYVAL states and territories where financial inclusion used to be more restricted.

***FS:** What results of Russia's presidency in FATF do you believe deserve being emphasized?*

J.R.: Seeing MONEYVAL ex-chairman Vladimir Nechaev as the FATF President was a great pleasure. I would like to say he fulfilled his duties in a habitually impressive manner – always with a touch of humor, which is not that usual in MONEYVAL. There were many achievements during the last year, but I would like to mention one that has already borne fruit. Vladimir wanted to pave the way to closer cooperation between FATF and Egmont Group, and he was in my view the first FATF President to ever pay attention to EG during his term. I think this gesture of support to Egmont Group was rather late. It was a pleasure to see that during the last FATF meeting we heard of plans and strategies of the Egmont Group immediately from its chairman. I believe it is a good sign because Egmont Group is a major player in AML/CFT. Today, with extended regional presence of Egmont Group and closer geographic alignment with some FATF-Style Regional Bodies, we in MONEYVAL expect closer cooperation with Egmont Group in the future. We anticipate learning more about their critical and analytical works through trainings and other events, which will significantly improve our reports and discussions.

***FS:** What are your impressions from the efficiency workshop that was held during the plenary meeting as the basis for the following round of assessment?*

J.R.: The next round of assessment will set new challenges, especially, for the states who wish to demonstrate their efficiency. The workshop was meant to increase awareness of immediate results and generation of some knowledge about the types of information that the countries may use to demonstrate their efficiency to experts.

The workshop was a part of the program of plenary meeting. In September, we covered three immediate results (3, 6, 7), and we are going to discuss the rest during the plenary meeting in December. It is a good method to suggest the way for the countries to get prepared and demonstrate their efficiency. Sessions were taken in a very positive way, and speeches were wonderful indeed. We have learned a lot. Presentations made by speakers were acclaimed and published at the MONEYVAL official web-site.

***FS:** What are your impressions from the report on Russia's Russia's follow-up report as a whole and from discussion thereof in particular?*

J.R.: From the moment of adoption of the third round of mutual evaluations and MONEYVAL second follow-up report, Russia have taken a number of measures with regard to surviving deficiencies under basic recommendations including amendments to AML/CFT Law and under by-laws. These amendments eliminated many deficiencies in preventive measures, although some are still in place.

Russian Federation also introduced some amendments to the Criminal Code of the Russian Federation. These amendments comply with the MONEYVAL recommendation of 2011 stating that financial threshold for «self-laundering» should be revised and eliminated, which is a considerable asset.

Progress on management of basic recommendations is obvious, and after the discussion the report was adopted in general. Russia's responses to questions asked by the reporting state of Austria and the plenary meeting received quite a high appraisal. I believe the plenary meeting was generally content with the progress achieved.

***FS:** What issues do you think Russia should take into consideration when getting prepared for the next round of evaluations?*

J.R.: In preparations to the next round of assessment, it is important to remember that the assessment process is mainly concentrated on efficiency. The Russian Federation will need to thoroughly think and decide how to prove to experts' efficiency of their AML/CFT regime.

An important element in demonstration of efficiency will be preparation of complex and reliable statistics that will be easily understood by assessors. Besides conceivable statistics, a brief but clear description of successful investigations and sentences, good examples of confiscation orders and restraining sanctions applied by the supervisory authority may color the country's responses to the assessment questionnaire. These examples may be used in the final report. Often, such exemplification of real experience is not observed in information provided to assessors. It is regretful, because provided examples may sometimes say more about efficiency than real statistics.

BANKING SECTOR

«JOINTLY WITH THE CENTRAL BANK WE ARE ARRANGING REMOTE MONITORING SYSTEMS»

The 8th Russian National Banking Forum titled "The new Russian banking system architecture: its competitiveness in Central and Eastern Europe" was held in Zadar (Croatia) on September 11-14, 2014

Evgenia N. Kalikhova
editor-columnist

The event was attended by Ambassador Extraordinary and Plenipotentiary of the Russian Federation in the Republic of Croatia Robert Markaryan, President of the Economic Chamber of Croatia Luka Burilovich, President of the Association of Russian Banks Garegin Tosunyan, Deputy Chairman of the Bank of Russia Vasily Pozdyshev, President of the Association of Croatian Banks at the Economic Chamber of Croatia Hrvoje Krstulovich as well as representatives of the relevant ministries and departments, heads of banks, and renowned scientists and experts in the field of economics.

On behalf of Rosfinmonitoring, the forum was attended by the Head of Rosfinmonitoring's Oversight Activities Department Olga G. Raminskaya. While highlighting the transparency of Russia's anti-money laundering system, its progress and recognition by the international community, O. Raminskaya emphasized during her report at the forum the importance of blocking the dirty criminal money from accessing the country's financial institutions. To do this, we need to introduce early warning mechanisms designed to help credit institutions avoid getting into difficult situations:

«We're working with the Central Bank on the creation of remote monitoring systems capable of identifying the use of shady and illegal schemes. Rosfinmonitoring's remote monitoring system, which consists of more than 75,000 registers of non-credit institutions and 1,057 banks, is designed to

monitor compliance by financial institutions with the AML/CFT law.

The central role in this system is played by financial institution as well as data submitted by it which, after being subjected to standard and cross sectional analysis using a specially designed and programmed mechanism, allows authorities to identify the most risky operations, schemes, industries, regions and entities. This is a product of the Risk Assessment Center which, at the request of the President of the Russian Federation and in cooperation with the Bank of Russia and law enforcement authorities, must play an important preventive role in cleansing the Russian economy».

O. Raminskaya spoke about mechanisms for monitoring customer migration processes occurring after the termination of the bank account by either the bank or the customer who is alarmed at the use of adequate compliance procedures:

«In line with the request of the Government of the Russian Federation, Rosfinmonitoring and the Bank of Russia have drafted a bill requiring credit institutions to report to the competent authority all cases of refusal to enter into a contract of bank account or termination of such contract by high-risk clients.

This bill also stipulates that the criteria for assigning customers to the high-risk category will be established by the Bank of Russia, while Rosfinmonitoring will maintain a list of persons whose requests for services have be rejected by banks. This list will be brought to the attention of credit institutions, which may take it into account when conducting customer due diligence, and will generally contribute to the full implementation of the most important international principal – «know your customer».

Olga G. Raminskaya

In addition, the event participants also discussed the competitiveness of Russian banks in Central and Eastern Europe, issues dedicated to the oversight of compliance with the AML/CFT law, the contribution of retailing to the capital market products with an emphasis on investment funds, the current status of the bill on the Financial Ombudsman, the problems of interaction between banks in Central Europe and Russia in the context of geopolitical instability, the issues of the banking audit in Russia, the regulatory challenges facing the Russian financial sector, etc.

SECURITIES MARKET AS ONE OF THE SECTORS MOST VULNERABLE TO ILLEGAL FINANCIAL TRANSACTIONS

The "shadow" sector of the economy is a permanent source of organized crime and corruption financing. Under control of the organized criminal gangs it generates its own infrastructure and financial area

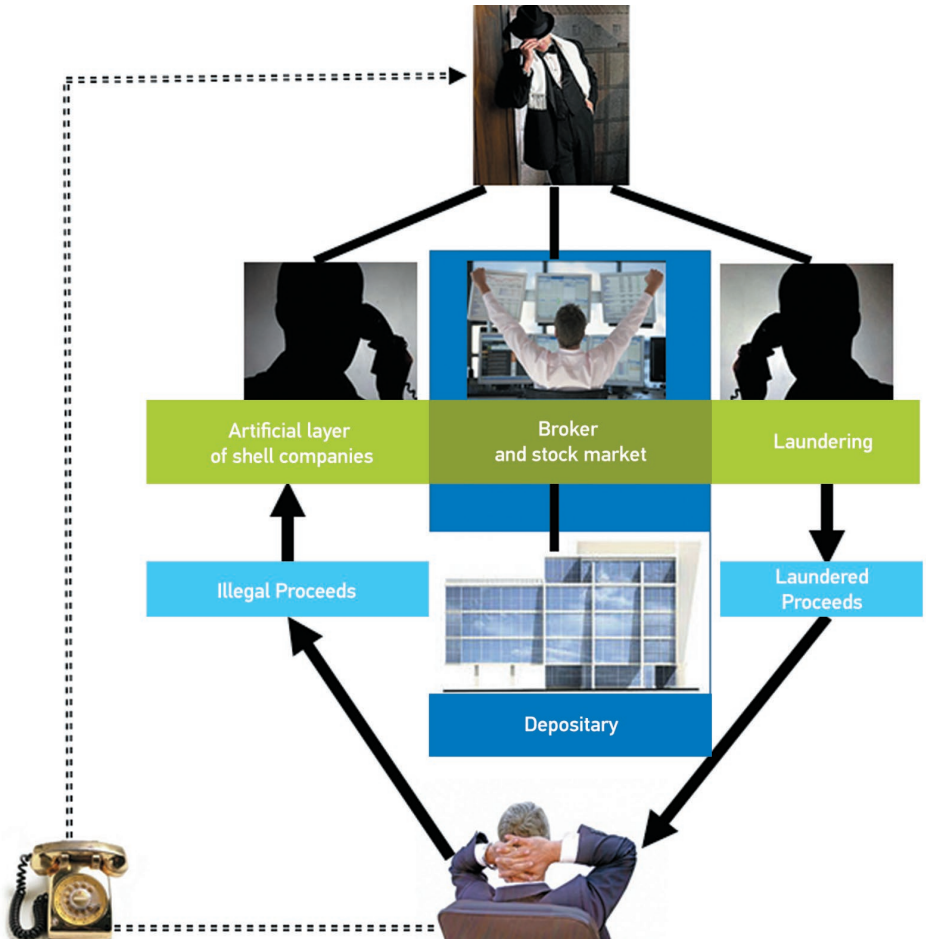
Ilya V. Aparyshev,
Class III State Councillor of the State Civil Service of the Russian Federation,
Lead Advisor of Macro-Analysis and Typologies Department
of the Federal Financial Monitoring Service

Ilya V. Aparyshev

Monitoring of current situation in the financial sector shows that the large "shadow" sector of the economy, emerged as a result of illicit cashing of funds and their further withdraw from Russia as well as due to the extensive use of shell companies, poses serious threat to economic security.

It has come under notice that illegal banking schemes increasingly shift to the non-credit financial institutions sector (securities market, insurance sector, etc.), which, among other things, is the result of "purging" the banking sector by squeezing out mala fide entities.

Figure 1. General aspects of the scheme and its main parties



It should also be noted that the rapid growth of the non-credit financial institutions sector is relatively recent and its regulation, as the global practice shows, is featured by high degree of liberalism.

At present, the securities market is considered to be one of the most vulnerable to illicit financial transactions, primarily related to withdrawal of funds abroad.

Comprehensive AML/CFT analysis of the professional securities market players has indicated that brokers and depositaries pose the highest threat[1].

Brokers are the entities engaged in circulation of securities, while depositaries are the entities engaged in accounting and recording of transfer of title to securities. In a situation where the same entity acts in the capacity of both broker and depositary, threat increases.

The conducted financial investigations have revealed that the utilized schemes are also

[1] FOR REFERENCE.

According to Federal Law No.39-FZ On Securities Market dated 22.04.1996:

- Brokerage activity involves carrying out civil-law transactions with securities and (or) entering into contracts being the derivative instruments on behalf and at the expense of a customer (including issuer of emissive securities) or in its own name and at the expense of a customer on the basis of repayable contracts made with the customer. A professional securities market player engaged in brokerage activities is called the broker.
- Depositary activity involves rendering services related to custody of securities certificates and/or accounting and transfer of rights to securities. A professional securities market player engaged in depositary activities is called the depositary. A depositary that makes settlement under transactions carried out on organized trade platforms in compliance with agreement entered into with the trade organizers and (or)with entities that perform clearance of such transactions is called the settlement depositary.

associated with a wide range of financial offences, such as tax evasion, illegal banking, establishment of shell companies, various frauds, etc.

The practice shows that, in the current economic situation, the professional securities market players, including brokers and depositaries, quite often get involved, directly or indirectly, in various illegal financial schemes for gaining extra profit. Such illegal activity is possible due to the liberal nature of the international regulatory framework and, as a consequence, soft and flexible national legislation (including laws and regulations pertaining to trade in securities) of most countries across the globe.

Illegal activities in the securities sector are the combination of well-coordinated actions of persons who have wide experience in investment operations and certain reputation in the stock market.

Below, we examine the money laundering typology scheme with the use of the services (engagement) of a broker and an affiliated[2] depositary.

Let us examine Figure 1 in detail:

1. A person (hereinafter referred to as the Client) has obtained illegal proceeds in result of, e.g. bank loan, insurance or IT fraud, deception of his counterparties, non-performance of government contract, illicit trafficking of precious metals and stones or drugs, VAT repayment, bribery, etc.

2. In order to launder such illegal proceeds (to make them legitimate) the Client approaches the money laundering scheme coordinator (hereinafter the Coordinator). Typically, the Coordinator offers well-proven schemes. However, he can design new ones in non-standard circumstances or when special requirements are set by the Client. In some cases, when the Client is not personally acquainted with (does not trust) the Coordinator, the Coordinator provides the security deposit in amount equal to the amount of funds to be withdrawn abroad. Provision of this guarantee increases the cost of the Coordinator's "service". This security deposit serves as some sort of insurance instrument for the Client, which is deposited or access to which is provided in the country where the Client resides or his affiliated entities are located, i.e. in the territory where illicit proceeds have been obtained. After the "service" is provided, the Coordinator closes this security deposit. Being subordinated to the Coordinator are the Performers responsible for three elements of the scheme, namely: "Artificial Layer of Shell Companies", "Broker and Stock Market" and "Laundering". Each of the Performers personally reports to the Coordinator and ensures smooth and rapid flow of the Client's funds through his stage of the scheme. It is important to note that in this ML typology a broker may willingly be engaged in the scheme or may just allow the Coordinator to use his services. **In both cases broker understands that he deals with funds of dubious origin.**

3. As agreed by the Client and the Coordinator the illegal proceeds flow through the "shell companies – stock market – laundering" chain, after which the Client has the laundered funds and the Coordinator and the Performers receive their profit.

Despite the relatively large number of parties and operations involved, the described mechanism allows for achieving the objectives of all stakeholders in a cost-efficient and rapid manner.

From the standpoint of the securities legislation, this scheme looks like legitimate one.

How one can conceal the origin of funds that are transferred to a broker?

Such concealment is ensured by the Performer in charge of the "Artificial Layer of Shell Companies" element of the scheme.

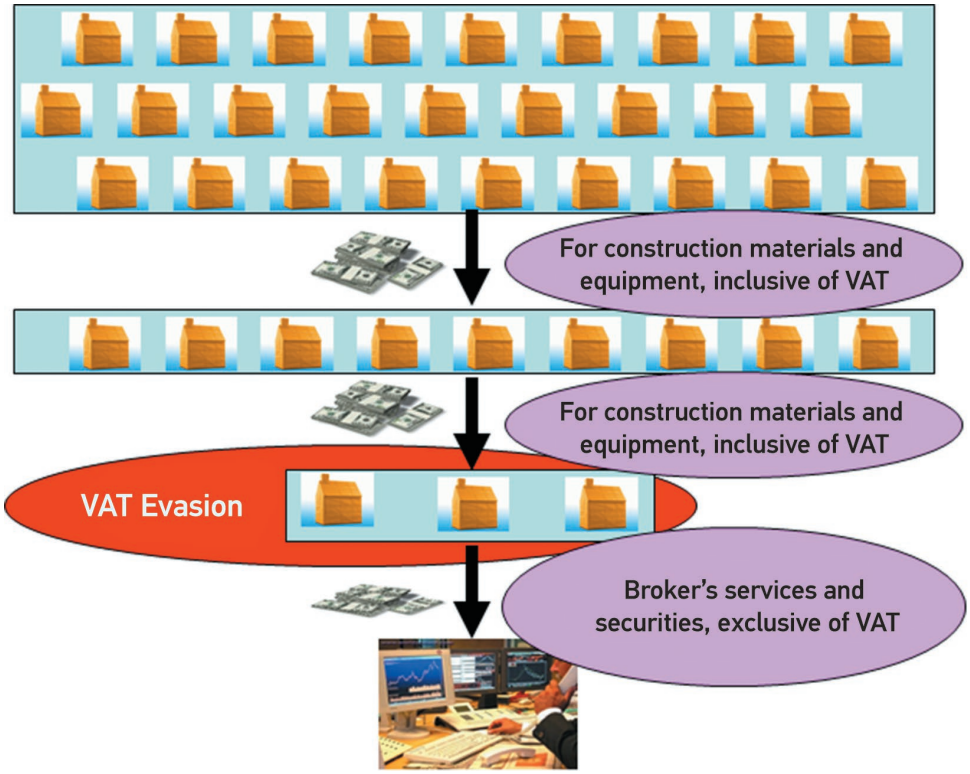
This element of the scheme (Fig. 2) includes a large number of shell companies that simulate business activity. Typically, the higher is the cost of the Performer's services, the thicker is the layer between the broker and the actually operational entity affiliated with the Client.

The number of shell companies on each level above the broker increases. In the presented example, the first layer consists of just 3 companies, the second layer includes 9 companies and the third layer is composed of 27 companies.

The mechanism is designed in such way that all parties involved look like independent business

[2] In this context, affiliation means association (contractual, corporate, brand-based or otherwise) of the broker and the depositary that pursue the mutually agreed policy.

Figure 2. Building the layer of shell companies evasion of VAT



entities engaged in trade in construction materials and various equipment that is subject to VAT at the common rate of 18 percent. However, all these trading operations exist just on paper.

This stage of the scheme is important since it is **at the first level where VAT is evaded**. The companies charge VAT on the goods they sell (i.e. the buyers pay the price that is inclusive of VAT, after which this tax is paid to the budget) and then acquire securities or brokerage services that are exempt from VAT. Thus, the tax is not paid or just partially paid to the budget.

In order to avoid inquiries form the government authorities, the shell companies used at the 1st and 2nd levels typically cease to operate after expiration of just one month (quarter) and are substituted by new ones. Such scheme necessarily functions on an on-going basis and allows its organizers to avoid, to a maximum extent, potential government sanctions.

Thus, the artificial layer of shell companies enables the Performer to completely disguise the Client's illicit proceeds that are transferred to a broker through this scheme and also allows him to evade VAT.

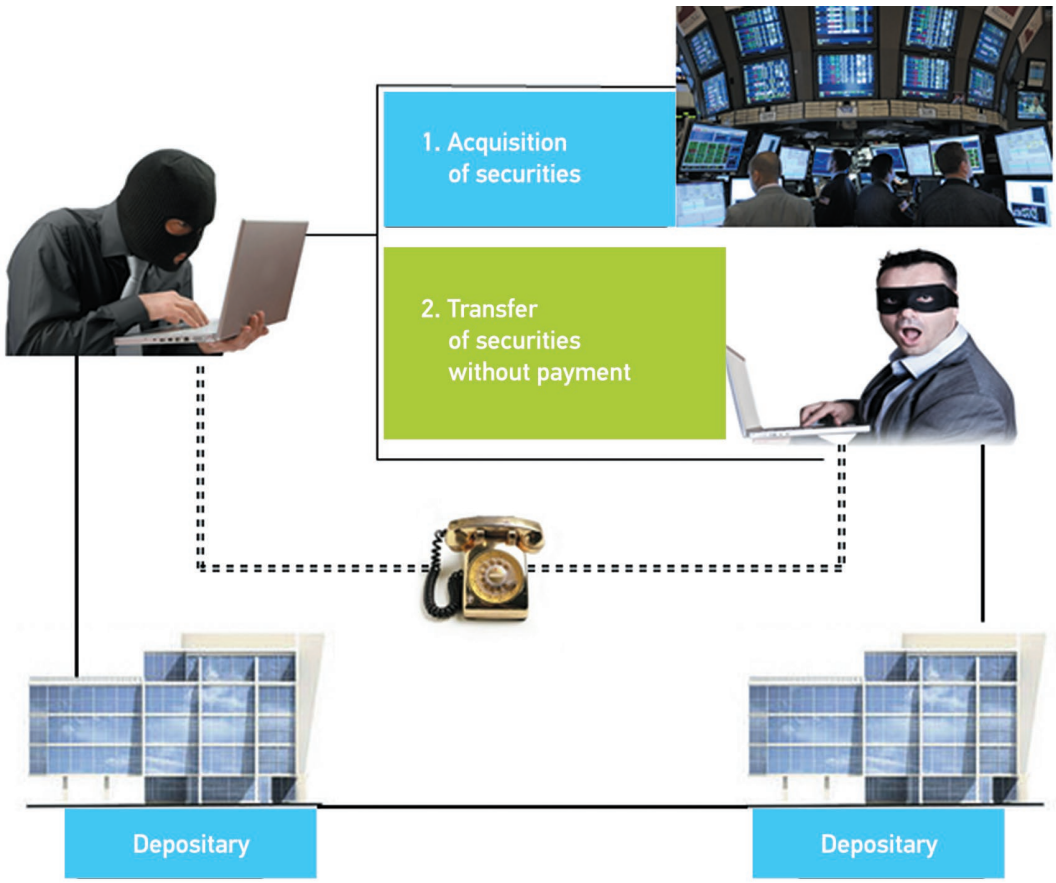
So, the Client's illicit proceeds are credited to the broker's account. **What are the next steps of the broker?**

At the instruction of the companies operating at the first level of the described layer, the broker purchases securities in the stock market and register them with the affiliated depositary. Typically, the acquired securities are the blue chips, i.e. the stock of well-known large companies featured by the stable performance indicators, which allow the investor to relatively quickly buy and sell them without exposing himself to high risk.

As shown in Figure 3, securities purchased by the broker are transferred, at the actual or fictitious instruction of the Client, to a third party (typically to other broker) in accordance with the prior arrangement without any payment, or are accounted on a depo account of the same broker. Such "transfer" may be disguised as debt repayment, gift, exchange, etc. The aforementioned third party broker, his client and depositary may be the residents of foreign country, including off-shore jurisdictions.

The securities are accounted with depositaries affiliated with the broker.

Figure 3. Acquision and convention of securities by broker. Bogus transactions. VAT evasion



It is important that, at this stage, the broker, **when receiving his fee, structures the scheme in such way that the securities are "transferred free-of-charge" within the same depositary**, which constitutes the grounds to consider such transactions as bogus ones.

After that, the third party broker sells the "unpaid" securities in the stock market.

As a result of all manipulations described above the Client's illicit funds come into possession of the third party broker.

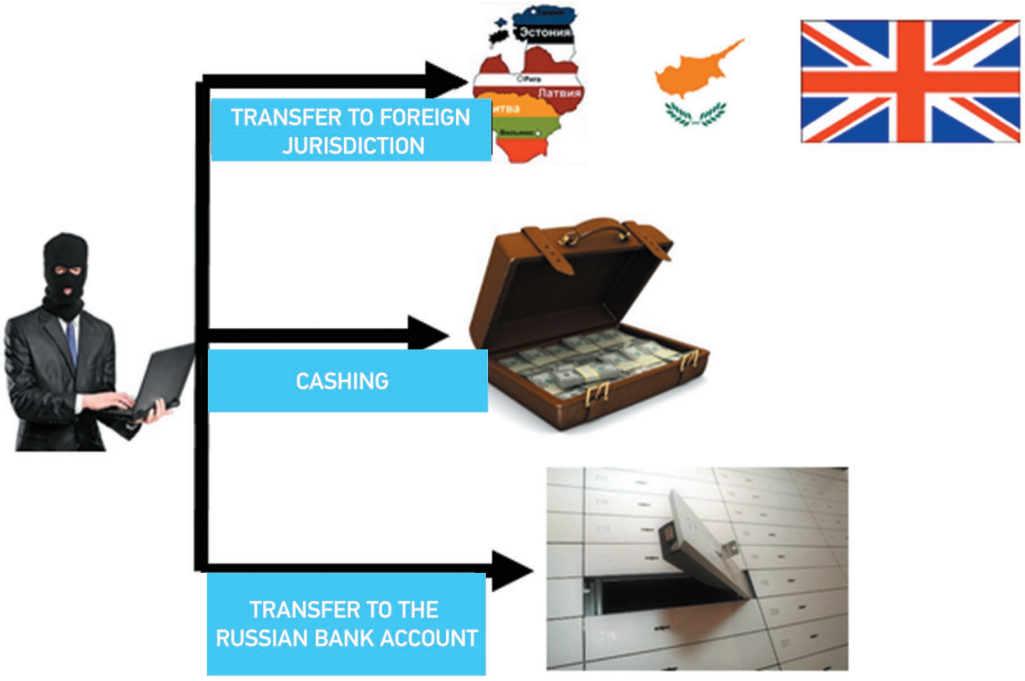
The broker, who holds the "unpaid" securities, either personally acts in the capacity of the Performer at the "Laundering" stage, or acts at the instruction of (is used by) the Performer. The utilized mechanism is similar to that used at the "Broker and Stock Market" stage.

As a rule, the funds, after flowing through the stock market chain, are transferred abroad to the bank accounts of entities affiliated with the Client. The most popular destination countries are Latvia, Lithuania, Estonia, Cyprus and countries under the UK jurisdiction.

However, in the current political and economic situation, the laundered funds often remain in Russia and are cashed out with the use of various schemes (including bill schemes), most of which have been designed abroad and involve foreign counterparties, or are transferred to the Russian bank accounts of entities affiliated with the Client. Besides that, such flow of funds require "long-term money" which are currently available to few banking institutions in Russia, This leads to a situation where the reserves of non-government pensions funds and other domestic savings are used in illicit financial transactions.

Finally, it should be noted that, despite implementation of enhanced controls, significant liberalization of investment activity under the international and national legal frameworks of

Figure 4. The scheme activities on laundering of proceeds from sale of securities



most jurisdictions across the world provides wide opportunities for laundering illicit proceeds. This indicates the need for paying special attention to the considered sector, especially in the context of the national risk assessment and preparation for mutual evaluations that will be conducted under the new FATF methodology which is primarily focused on effectiveness.

PRIVATE SECTOR

"KNOW YOUR CUSTOMER" AND FATCA

July 1, 2014 passed – it was the date of coming into force of the first notable requirements of the US Foreign Account Tax Compliance Act – FATCA, which still raises much talk and concerns in financial community

Dmitri V. Chistov,
Head of Risk management Department KPMG Russia and the CIS

Dmitri V. Chistov

We should note that FATCA is not the only initiative for tax control and information exchange in the world. In European Union, the issues of information exchange, tax withholding, participation of foreign tax bodies in tax audits and other aspects of tax cooperation have been governed by the EU Directives On Administrative Cooperation in Taxation 2011/16 (previously – On Mutual Assistance in Tax Issues (79/799) and On Savings Taxation (2003/48), On the General System of Interest and Royalty Taxation (2003/49), etc.) for more than 10 years already. At that, the principles of information exchange and withholding justly apply to the EU member states as well as a number of third countries such as Switzerland, the Channel Islands, and offshore territories of the Caribbean Sea.

Another international tool in the sphere of tax collaboration is the OECD Multilateral Convention[1] on mutual administrative assistance in the tax field, which implies automated information exchange, multilateral simultaneous tax audits and international assistance in collection of due taxes. As of today, tens of countries and territories – including Azerbaijan, Georgia, Moldova and Ukraine – have ratified the OECD Convention. The Russian Federation is in the process of approval, and it will issue its first report as part of this system in 2018.

Thus, it is clear that the US FATCA is neither the first nor the last initiative in this line. However, it is the first one to introduce the practice of mandatory withholding of 30% tax in case of non-participation, and it actually forces the parties into cooperation. At the same time FATCA - just as other initiatives – stipulates the right of cooperating countries to receive information about their citizens.

The Tax Code of the USA already determines the procedure for international cooperation with regard to taxation and regulation of investor payments (dividends/interest) in financial instruments of the USA. This procedure is regulated by chapter three of the Tax Code and implies conclusion of an agreement with a foreign financial institution and provision thereto of the status of Qualified intermediary (QI). Chapter four of FATCA is the logical continuation of chapter three of the US Tax Code (QI), its objective is finding American investors who "hide" in other states including those in the form of corporate entities (QI does not go beyond the level of legal entities). Technically, FATCA – unlike, for instance, FCPA[2] – is not an extraterritorial law. It suggests foreign financial institutions voluntarily join and enter into an agreement with the US Internal Revenue Service (IRS), but also binds financial institutions who are subject to FATCA to withhold 30% of payments from annual and recognized income associated with the USA (Fixed Determinable Annual Periodical (FDAP) Income) to the benefit of Non-Participating Foreign Financial Institutions – NPFFI, Limited FFI – LFFI, and customers who have refused to be governed by FATCA. Based on the above, we may assume that involved financial institutions will either withhold 30% from payments that in their view may be associated with receipt of FDAP Income, or – in order to avoid unnecessary trouble – even terminate correspondent relations with non-participating financial institution.

Thus, financial institutions whose activities in any way relate to the USA have virtually no choice except for termination of such activities, and since financial market established in the USA is the most efficient, capacious, comprehensible and as a result attractive, the USA use this fact in order to persuade institutions into helping them with their tax problems.

The purpose of FATCA is search for American citizens – U.S. Persons who evade taxes.

Key FATCA requirements to foreign financial institutions are new approaches to customer identification, reporting, withholding of penal taxes as well as regular monitoring and control of adopted measures. New principles of identification of individuals (organization clients) and detection of U.S. Persons among them came into force on July 1, 2014 (for legal persons it will take effect on January 1, 2015). Sanctions pertaining to mandatory withholding of 30% will apply from the same date, and the first report to the Internal Revenue Service shall be sent before March 31, 2015.

We would like to undeceive those who believe that an account is a key object of FATCA analysis. In fact, analysis is focused on a customer, and thus on the process of identification or a wider "Know Your Customer" concept, proper forming of which will determine further efficiency and correctness of measures taken. That is why the key subdivision to receive the main load is the department of compliance, AML/CFT or financial monitoring, since integration first affects the processes of customer identification and analysis, and further – monitoring, too.

FATCA determines the aggregate balance threshold at $50,000 for individuals and $250,000 – for legal entities, with no identification of existing customers required by FATCA within these limits. However, bearing in mind that the customer is primary, it seems reasonable for comparatively small financial institutions with the minimal number of abandoned

[1] The Organisation for Economic Co-operation and Development (OECD).

[2] Foreign Corrupt Practices Act.

accounts to classify a customer in relation to his FATCA status irrespective of the balance of his accounts, and then monitor his aggregate balance – FATCA allows doing this. We would also draw your attention to the concept of "financial account" introduced by FATCA. It is not just a banking account in the Russian meaning, but a wider Western notion of "account", which sometimes implies the customer organization as such. According to FATCA, "financial account" except for deposits comprises custody accounts, annuity or surrender insurance contracts, participation in equity or borrowed capital. Exception is made for some saving accounts including pension accounts with annual installments not exceeding $50,000, insurance contracts with determined conditions, escrow accounts.

Situation in Russia and the CIS

Legislative regulation of FATCA requirements is currently an urgent issue to financial organizations of Russia and the CIS. Everyone except Russian financial institutions impatiently waits for news about actual execution of mostly approved intergovernmental agreements, new explanations, recommendations and regulations, pursuant to which fulfilment of FATCA requirements will not expose financial institutions to risk of violating the local legislation on data transfer, customer identification, closing of accounts and reporting.

Most states of the post-Soviet area work on implementation of FATCA requirements. Among those, we may single out activities pursued by Azerbaijan, Belarus, Georgia, Kazakhstan and Ukraine, in negotiation of intergovernmental agreements and elaboration of internal control rules.

Unfortunately, Russia and the USA failed to concert the intergovernmental agreement concerning implementation of FATCA, and Russian financial organizations have to make agreements and deliver information to the US Internal Revenue Service directly. Of some help in this regard should be Federal Act No. 173-FZ that eliminated certain discrepancies in legislation of Russia and the USA, which could prevent Russian financial organizations from fulfillment of their obligations under FATCA.

It is worthy of note that in Russia information exchange under FATCA is considered in the general

context of measures taken for the purposes of exchange of tax data as part of joining the OECD Multilateral Convention on mutual administrative assistance in the tax sphere, economy de-offshorization measures. A range of bills aimed at implementation thereof already exists. Thus, it becomes clear that identification of customers who are foreign tax payers will not be limited to FATCA implementation.

Globally, intergovernmental agreements have been already concluded by 42 countries[3], five of which have been executed under the second model, the rest – under the first model. Many states are still in the process of negotiations and probably because of that IRS offered to recognize a state as the FATCA participant immediately after execution of the intergovernmental agreement, before its ratification; besides, IRS grants all rights to the signing country after ratification of the agreement – there are 39 such countries, with 31 of those having ratified the agreements according to the first model.

Financial Institutions' Objectives Pertaining to FATCA Implementation

In the current situation, in order to minimize risks of the Russian financial institutions, it seems reasonable to proceed from the following:

1. Financial organization should assess the nature and amount of risks that may arise from its failure to meet FATCA requirements, and shall consider the number and extent of operations performed by the credit institution and subject to control under FATCA, the number of customers meeting established FATCA criteria, extent of operations performed via the US credit institutions, etc.

It makes sense to perform such risk assessment at high management level with employees of tax and compliance divisions, internal control service and external consultants engaged.

[3] Intergovernmental agreements according to the 1st model were executed by Great Britain, Hungary, Germany, Denmark, Jersey, Guernsey, Mauritius, Malta, Mexico, Netherlands, Norway, Isle of Man, Ireland, Spain, Italy, Cayman Islands, Canada, Costa Rica, Singapore, Finland, France, and according to the 2nd model – with Switzerland, Japan, Chile and Bermudas.

When considering application of FATCA requirements, the organization should first answer a number of essential questions:

- is the company a foreign financial institution (FFI)[4];
- what financial accounts does the company have;
- are there any indicators that any account holder is a Specified US Person;
- does the company have any accounts that are subject to reporting after application of necessary identification and customer due diligence measures.

2. Advisably, having determined its own FATCA status based on analysis specified in cl. 1, the financial organization should take a number of strategic decisions concerning participation or non-participation in FATCA, registration at IRS portal, allocation and appointment of Responsible Officer/ Point of contacts, establishment of implementation project group, appointment of project manager, obtaining external consulting/IT or other help, approaches to work with recalcitrant customers[5] and non-participating financial organizations.

3. If a decision to participate in FATCA is made, immediately start elaboration and implementation of necessary changes in internal processes of financial organization, and technological solutions that will be required in order to detect and collect necessary information. Based on this registration, IRS assigns FATCA identification code (GIIN) that will serve many purposes including comprehension of FATCA status (friend-or-foe).

4. In any case, it is recommended for the financial organization to obtain formal definition of its status within the FATCA framework as soon as practicable in order to avoid possible penal withholdings. In particular, existing customers should be classified, new customer identification procedures should be officially introduced including elaboration of new procedures of client service and interaction for the front office, client documentation should be updated, IT-systems and databases should be modified and brought in compliance.

5. From July 1 until the end of 2014, organizations will have time to adjust submittal of annual reports to the US tax authorities and withholding process. It should be noted that withholdings process may be kept to a minimum by delegation, i.e. transfer of withholding right to the senior organization in the payment system, for example, to an American or European bank. At that, withholding will hardly affect recalcitrant customers since there will be none in the organization for one simple reason – from 2010 when the act was adopted, wealthy and long-headed tax evaders in the USA have had an opportunity to study the requirements and – most probably – to alter their investment and cash flow algorithms. So, those who wanted to hide have already done so, while expats working in Russia and other law abiding tax payers will apparently be the first to declare their relations with the USA.

Who Will Prepare Financial Market Organization to FATCA

Our experience shows that the most advanced in application of FATCA were financial market organizations that appointed to the position of the responsible officer a manager of quite a high rank to "flash" the efforts of the FATCA working group with his influence and knowledge. However, routine work fell to project managers – either project management professionals or, which is more often, specialists in anti-money laundering and combating the financing of terrorism (AML/CFT) or their "neighbors" from compliance division. The leading role of AML/CFT specialist seems justified because – despite the presence of the word "tax" in FATCA name – the entire history is in provision of support to the US Internal Revenue Service in search of abusive tax payers and never in monitoring of elite operations or informing the CIA of the results. Obviously, in order to find these Americans, one should know its customers, which is

[4] FFI – any foreign (non-U.S.) legal entities including: banks and other organizations that perform banking operations; depositories; organizations that provide safe custody services; investment companies (including collective investment funds, hedge funds, mutual investment funds, direct investment funds, venture capital funds, majority holding buyout funds, etc.); insurance organizations or holding companies that issue or perform payments under annuity or surrender insurance contracts; holding companies or treasurer's offices.

[5] Recalcitrant account holders – are customers who have refused providing any documents to prove existence or lack of the U.S. Person status.

the strong point of AML/CFT specialists who make "know your customer" procedures work.

AML/CFT specialists direct operation of the entire system – they know the whole process from filing of account opening application to the rules of storage, update and testing of customer information. AML/CFT specialists usually know the systems used in automation of the process of documenting, storage and systematization of customer information, which means they can professionally answer many questions associated with FATCA implementation. For instance, elaboration of certain questions for the new clients that will help detecting indicators (criteria) of U.S. Persons established by law will be absolutely natural.

Now, a few words about relations between AML/CFT division and compliance service. Leaving aside Russian subsidiaries of foreign banks, in which compliance service with seamlessly integrated AML/CFT division has been in place from the very beginning, according to international practice, we would like to discuss purely Russian banks in greater detail. Here we can observe the entire range of organizational decisions from mature elite AML/CFT division that has been headed by AML/CFT "patriarchs" for over 10 years now (from the day of coming into force of AML/CFT law in 2002) and moderately joining compliance division sometimes shyly calling itself "international compliance" – probably in order to emphasize introduced, foreign nature of the division established to "please" foreign partners – to orderly and consistent compliance service that seamlessly and naturally incorporates AML/CFT division like the one we can observe in Sberbank.

As we can see, with entry into force of the new edition 242-P, many of our clients choose the denomination "compliance service" (leaving aside the other strange and confusing name suggested by 242-P "internal control service" – control is by far not the main function of compliance division). Further, pursuant to common international practice, this relatively new service accommodates the existing service elements, for instance, professional participant's controllers and certainly the AML/CFT subdivision. In such cases, we can say that the compliance service is the leader in preparation of the bank to FATCA, which shall be regarded as a successful decision.

REGULATION AND SUPERVISION

PRACTICE OF IMPLEMENTATION OF THE FEDERAL LAW NO. 134-FZ BY CREDIT INSTITUTIONS OF THE SIBERIAN FEDERAL DISTRICT

Sergey Yu. Nekrasov,
Deputy Head of the Inter-regional Department of Rosfinmonitoring in the Siberian Federal District

Sergey Yu. Nekrasov

With entry into force of Federal Law No. 134-FZ, banks gained the right to refuse an individual or a company in processing transactions which are suspected to be aimed at laundering of criminal assets or financing of terrorism.

Alongside with that, banks are now entitled to make a decision on termination of the contract of bank deposit, account, if the customer is found to perform suspicious transactions several times. And if banks initially realize that the customer (company or individual) will most probably carry out suspicious transactions, then the credit and financial institution is fully entitled to refuse making a contract of deposit/account with such customer. Herewith, banks also acquire a new obligation – the law binds the banks to inform Rosfinmonitoring of all cases of refused customer service.

In the Siberian Federal District, credit institutions started widely and actively using their right to deny service to customers who carry out suspicious transactions from November 2013, upon coming into force of the departmental regulation of the Bank of Russia – Decree of 23.08.2013 No. 3041-U Concerning the Procedure for Submission by Credit Institutions to Competent Authorities of Information about Denied Execution of Bank Account (Deposit) Agreement with the Customer, Refusal to Execute the Customer's

Order, and Termination of Bank Account (Deposit) Agreement with the Customer on the Initiative of the Credit Institution – that was adopted in elaboration of the federal law. However, implementation of the right to refuse may be called wide and active only conditionally – as compared to previous periods when such activity was close to zero. Against the background of general rise in the number of bank operations, the share of denied operations remains negligibly small.

At that, analysis of reports on denied customer service received from credit institutions operating in the territory of the Siberian Federal District in pursuance of the adopted law demonstrated that by far not all banks used the granted right. Only about a half of regional banks and less than one third of branches operating in the district have used this right by now. Although this statistics is indicative of higher activity of Siberian banks as compared to other federal districts where banks use their right of refusal even less enthusiastically, it is only every ninth bank that ventures to do so throughout Russia.

This fact may imply at least three options of explanation. Either most banks no longer have bad customers and they had got rid of clients that bore the risk of illegal financial operations even before law 134-FZ took effect. Or most banks make away with suspicious customer without informing competent authorities. As one of bankers said, the banks that value their reputation and avoid working with obviously suspicious clientele take a beaten track of diplomatically offering a customer to close the account on his or her own initiative. A third option is possible – banks that earn from suspicious transactions neither refuse service to their clients nor inform Rosfinmonitoring, which means they work in the same way they used to before Federal Law No. 134-FZ was adopted, thus bearing reputational risks and risks of being sanctioned by regulating authorities.

Among reports of Siberian banks on denied customer service, reports on refusal to execute bank account agreements make up the bulk (almost three fourth of total amount). It proves that in implementation of their power to refuse bank servicing, credit institutions prefer parting from the customer even before opening an account where high risk level is present. Herewith, in 70 per cents of cases, when stating the reason for refused execution of bank account agreement, banks specify suspicions that conclusion of such agreement is performed for the purposes of money laundering or financing of terrorism. In 30 per cent of cases, the reason is the customer's failure to provide identification documents. Some reports describe single cases of refused opening of accounts due to the absence of the person opening the account or its representative.

As for refusals to execute customers' orders, this type of rejections constitutes less than one fourth of total number of registered refusals. In most cases (80 per cent), the reason is in suspicions of employees of the credit institution that the operation is carried out for the purposes of money laundering or financing of terrorism. Other refusals to carry out a transaction owe to failure to provide the required documents.

Reports on termination of bank account (deposit) agreements are not that many, with their share in the Siberian Federal District making up about one per cent. Credit institutions apply this measure of last resort in exceptional cases when two or more order rejections occur in relation to one client within a calendar year. However, this category of customers bears the highest risks of illegal financial operations and deserves high attention on behalf of supervisory authorities and sometimes law enforcement agencies. After termination of the bank account agreement in one bank, they transfer funds to other banks and continue their suspicious transactions. Cases were discovered where some individual customers had over a hundred of accounts with tens various banks. Anyway (this is also proven by analysis of banks' reports on denied service), having been rejected in one, another and even a third bank, such high-risk customer sooner or later finds a bank ready to provide banking service and perform suspicious operations of the client. The same refers to banks that keep servicing customers with two or more rejections and are in no haste to get rid of such customers.

All of it one more time emphasizes the necessity to develop a bill that implies establishment of a public list of suspicious bank customers – individuals and companies that were denied bank servicing. This being the case, the customer – individual or organization – entered in the grey list should not fully lose its right to bank servicing, otherwise its rights will be violated. The client will have no chance to rehabilitate and comply with law, which will force the client to "shadow" segment of transactions, to cash settlements, thus creating even higher risks to financial sphere.

VIRTUAL CURRENCY

BITCOIN OWNER IDENTIFICATION POSSIBILITIES FOR LAW ENFORCEMENT AGENCIES

A virtual currency can be defined as a digital representation of a value that functions as a medium of exchange, within a specific virtual community, such as a specific Web-site (regulated exchange markets) or user network with specific software to monitor virtual currency

Elena S. Macogon,
a Student of Financial University under the Government of the Russian Federation

Elena S. Macogon

Bitcoin Transactions Mechanism

Bitcoins are created and put into circulation, using a process called «mining». After downloading and automated interactive installation of software for using the Bitcoin system (free software downloaded directly from the Net), offline update takes place of all transactions made at various nodes of the network. The application also provides for the creation of a bitcoin address consisting of a random sequence of alpha-numerous combinations (33 characters on the average), which always begins with 1. In doing that, the users are allowed to have an unlimited number of bitcoin addresses.

To send bitcoins, their number and the address to perform transmission should be entered. The user's computer signs the digital transactions and performs information transmission in the distributed Bitcoin P2P network. At this stage, it is also confirmed that the sender of bitcoins is their immediate owner at the moment. After that, the receivers can process the received bitcoins. Usually, this procedure takes a few minutes and is irreversible. The Bitcoin software controls the speed at which bitcoins are created, but not the market value of bitcoins, which is determined by several factors: people wish to buy bitcoins; opening of a criminal investigation by the law enforcement agencies against a number of participants who employ criminally the anonymity features of bitcoins; hacking attacks from distribution of untrue information to theft of bitcoins from those who make transactions.

Beside bitcoins mining, the users can also purchase bitcoins that are already in circulation, by receiving them as a present or payment for goods or services, by buying them in bitcoin kiosks (sometimes called bitcoin ATMs) or by buying at third-party platforms. The rest of bitcoins is stored at cryptographically protected bitcoin addresses of the users. When the users transmit bitcoins, the receiver sends a bitcoin-address to the sender, and the sender permits the transaction, using a private key (that is, a secret code which allows the sender to control his or her bitcoin-address). Only a bitcoin address is required for completing the transaction that does not contain any personal information. Bitcoin transactions do not require the sender or receiver to disclose their personality. Personal identification in the use of bitcoins is additionally made difficult through the use of pseudonyms by the bitcoin transaction participants, the number of pseudonyms being unlimited.

Bitcoins can be both exchanged for a real currency and used for purchasing goods or services in a real or virtual space.

Legal Regulation of Bitcoin Transaction Makers and Participants in Russia and Foreign Countries

It is important to note that banks from over 30 states have already issued a warning on the use of crypto-currency. However, a number of countries have tried to introduce Bitcoin in the legal sphere, which consists in the following: requirements appeared for licensing or registration of that activity and for conducting business in accordance with the legal regulations. Various sanctions can be imposed for violation of

those requirements, up to bitcoin currency exchange office account freeze for absence of a license as in the USA. For example, in New-York, licensing and regulatory requirements have been developed for each individual virtual currency exchange office. In the State of Texas, a memorandum has been issued that describes how the current licensing requirements cover the virtual currency. In Germany, so far there is no apparent need for licensing, but it can become necessary under certain circumstances. FinTRAC of Canada (counterpart to Russia's Federal Financial Monitoring Service) has circulated letters to a number of large national bitcoin service operators stating that their transactions are covered by country's anti-money laundering laws and are subject to registration with FinTRAC. Under the French court decision, already since 2011 bitcoin currency exchange companies shall be considered as payment service providers and subject to supervision by the state authorities.

Besides, a number of countries where bitcoin is an object of taxation (when the virtual currency is exchanged for goods or a real currency) require that bitcoin transaction records must be included in accounts and records. In the USA, Australia, Bulgaria, Norway, Sweden, Germany, Singapore, Finland, Canada, Great Britain, Switzerland, taxation of bitcoin transactions is regulated, but to a different degree of detail and conditions at which taxable income or negative return is formed.

Disputes regarding the status of Bitcoin arise in some countries that are solved through legal proceedings. For example, in the Netherlands, the court directed in May this year that Bitcoin is an exchange medium and acceptable payment method in the country but cannot be defined as a legal means of payment (a real currency or electronic money). In some countries, laws regulating payment systems and electronic money do not cover Bitcoin.

In accordance with article 27 of Federal Law «Concerning the Central Bank of the Russian Federation», ruble is the lawful currency of the Russian Federation. Introduction of other pieces of money and issue of quasi-money (which includes Bitcoin) is prohibited in the Russian Federation. Federal Law No. 110-FZ «Concerning amendments to a number of legislative acts of the Russian Federation» of 05.05.2014 has increased legislative pressure regarding the use of non-personified (anonymous) means of payment. However, Bitcoin and other crypto-currencies are not covered by this law. That's why the Ministry of Finance is currently developing a draft law regarding prohibition of transactions with quasi-money (including cryptocurrencies) covering the use of quasi-money as a means of payment or to exchange for rubles or foreign currency, with the possibility of criminal or administrative prosecution of the participants.

Investigation of Bitcoin Transactions Participants - Plan of Actions for Law Enforcement Agencies

It must be said that the Russian Legislation gives to the law enforcement agencies a rather wide armoury of methods regarding the opportunity to identify the participants of criminal transactions with bitcoins. In accordance with the Federal Law 126-FZ «Concerning Communications» of 07.07.2003, to identify a participant to a bitcoin transaction, criminal investigation department officer can request data from the Internet service provider, regarding the person of interest (including data on the communication services provided, which possibly can allow the officer to establish the frequency and time of Internet connections). The additional information required for identification can be gathered using Internet Forensics. The value of Internet Forensics lies in the fact that it allows reception of evidence even without access to the offender's computer, based on investigation of «information traces» in the network alone. It should be noted that the findings of Internet Forensics underpin the evidential base as they allow demonstration of the fact that additional networking devices or expanders have been added on the server or workstations and demonstration of the facts («traces») of using external (third-party) software. This is highly important, because software must be downloaded to make transactions with bitcoin. Besides, some individuals prefer to store bitcoins on their workstations (on the hard disc drive of their computer or laptop). Also, Internet Forensics allows determination of:

- internet addresses accessed from the given computer hardware, as well as data proving the use of credit cards for payment or conducting of other electronic payments;
- messages received (sent) by using e-mail or personal Internet communications service software, and the content thereof;
- data on the access to remote resources on other computers or servers by the users of the given computer, their parameters and attributes (user names and passwords, provider's data, date and time of connections etc.)

However, the maximum possible information should be gathered and contact should be established with the suspect before Internet Forensics. For instance, items 4 and 5 of article 15 of federal Law № 144-FZ «Concerning operative-investigative activities» of 12.08.1995 allow the law enforcement agencies to set up companies, use documents paraphrasing the names of officials, departmental identity of enterprises, premises or transportation facilities, as well as the identity of citizens assisting the law enforcement agencies on the confidentiality basis. The police investigator may appear as a company manager wishing to purchase the product (which has been fictitiously written off or withdrawn from current assets in any other way, according to information collected), or request additional information required for conducting a transaction from a person involved in illegal business practices without registration with tax authorities, in exchange for bitcoins.

As it is quite difficult to determine the exact time when the user entered the network for conducting a transaction, then the police investigator, in accordance with article 64 of Federal Law No. 126-FZ «Concerning communications» of 07.07.2003, may approach the company providing Internet services to the person of interest to temporarily suspend the Internet services based on a reasoned decision in order to synchronously enter the network and establish a contact with the person of interest.

The Parties to Bitcoin Transactions - Identification Possibilities and Complexities

How can it be proved if at all that a transaction is being concluded exactly with the person of interest? All transactions are registered in blockchain (a public book) which contains data on bitcoin addresses,

including the transaction date, time, and amount. Of course, this information can by no means identify the person of interest; however, there already exist methods for identification of persons involved in certain bitcoin transactions (by investigating the transaction clusters between specific addresses). On the Web-site https://www.usenix.org/system/files/login/articles/03_meiklejohn-online.pdf, information appeared in December 2013, describing the way how the address can be changed in a transaction so that to prevent the person involved in the transaction from knowing about the transaction (except when this person investigates the network unit manually), and analyzing the possibilities of limiting the Bitcoin anonymity on the whole. Besides, the client information can be registered, if person exchanges dollars for bitcoins, and this information in combination with blockchain allows determination of authenticity of the participants to a bitcoin transaction.

In the light of the above, it is necessary to stress that a necessity exists of involving an IT specialist as the police investigator establishes a contact with the person of interest in the network, in order to prevent loss of data that can appear as evidence during the criminal trial.

Currently, the following techniques have been developed to enhance the confidentiality of virtual currency exchange transaction participants:

1) BitcoinBath and BitLaundry, allowing reception of payments from several users, which makes it difficult to identify the participants through blockchain;

2) use of alternative virtual currencies, such as Zerocoin or Anoncoin;

3) anonymous networks for hiding the real Internet addresses of users, using special software, such as The Onion Router (TOR), I2P.

4) creation and use of a new bitcoin-address for each incoming payment;

5) use of third-party electronic wallets that allow users to consolidate a lot of bitcoin-addresses, as well as to store bitcoins and easily get access to them from any device.

However, the store of bitcoins by third-party services can involve a lot of risk. It should be noted that online Web wallets can feature various degrees of antihacker protection, which are not always adequate. Hackers can spam via e-mail (in order to manipulate prices on the market), disseminate viruses (via «Infostealer. Coinbit» – the first malicious software designed for bitcoin pilfering from hacked bitcoin wallets of the users) and hack data bases (for accessing user names, e-mail addresses, and hash passwords for thousands of users). There has been a case when a bug in the software allowed making a change in the bitcoin transmission transaction data that cause it its turn claiming to return of the funds. Sometimes malicious software can be propagated through links put in social networking services. Also, quite often the established cash withdrawal limit per day appears as limitation for hackers.

EDUCATION AND SCIENCE

ADVANCED TRAINING FOR LECTURERS OF AML/CFT NETWORK INSTITUTE

During the second half of May 2014, the Board of a Network AML/CFT Institute (the Network Institute) decided to define specialities and majors of educational programs of higher education for training of future employees of the national anti-money laundering system

Marina I. Makarova,
ITMCFM Project Manager

Availability of field-oriented educational programs and professional standard of AML/CFT specialist is not enough to implement personnel training programs. Undoubtedly, professional standard meeting modern requirements and educational programs will be used as a foundation for development of higher education system. Yet, the primary task is training of highly qualified teaching staff. The Network Institute needs lecturers who possess field-oriented knowledge about specifics of education of staff for the national AML/CFT system.

Considering the many years' experience in training of lecturers to teach specialists of financial and non-financial organizations liable to take AML/CFT measures, the ITMCFM have elaborated an educational program "Advanced Training of Staff in Anti-Money Laundering and Combating the Financing of Terrorism.

In order to train employees of the national AML/CFT system, the International Training and Methodology Center of Financial Monitoring held the advanced training course under the new program in October 2014. All educational institutions - members of the Network Institute - sent their lecturers to attend the pilot course. It was the first time that the ITMCFM trained lecturers from educational institutions of the Crimean Federal District. Thanks to videoconferencing, the training course was also attended by specialists from FIUs of Belarus, Kazakhstan, Tajikistan and Uzbekistan.

Significant part of the program is dedicated to studying of legal and institutional basics of the international AML/CFT system. Participants learned about the role of the Federal Financial Monitoring Service in the national anti-money laundering system. Specialists of the Service demonstrated financial investigation methods, specifics of typology studies. The issues of prosecutor's supervision were discussed with the representative of the Academy of the General Prosecutor's Office of the Russian Federation.

As higher education system in the sphere of AML/CFT evolves, formation of the resource base may not be underestimated. The ITMCFM provided students with access to the unique AML/CFT library. Lecturers also had an opportunity to use the Center's electronic training courses during their studies.

Having assessed the results of final performance review and analyzed students' questionnaires, we may conclude that advanced training under ITMCFM programs was a positive experience. In 2015, the Center is going to continue education of lecturers of the AML/CFT Network Institute.

TRAINING FOR SUPERVISORS

Specialists from Assay Chamber of the Russian Federation, Central Bank of Russia and Federal Tax Service have been trained the ITMCFM

Anna V. Bulaeva,
Correspondent

Supervision is one of the main instruments used for assessing effectiveness of the Russian AML/CFT System. Inspections and reviews conducted by the supervisors ensure quality and relevance of information on financial transactions. Findings of the inspections and audits of the supervised entities are the additional source of information used for conducting financial investigations and performing other analytical work for the AML/CFT purposes.

Training of the Assay Chamber Staff on Legal Regulation and Current AML/CFT System Development Trends

The Russian State Assay Chamber under the Ministry of Finance of the Russian Federation is the federal government agency empowered to conduct federal assay supervision and government control over exportation from Russia into the Customs Union non-member countries and importation from these countries into Russia of precious metals and precious stones and also to monitor compliance with AML/CFT legislation of the Russian Federation by entities engaged in sales and purchase of precious metals and stones, jewelry made of them and scrap.

On September 15-16, 2014, the workshop on important issues of legal regulation and current AML/CFT system development trends was held at the International Training and Methodology Center for Financial Monitoring (ITMCFM) for the Russian Assay Chamber staff.

The workshop was arranged and held for raising awareness of the attendees about AML/CFT regulation and supervision, briefing them about main changes and modifications in the Russian AML/CFT legislation and informing the participants about typology exercises and outcomes of cooperation between the Assay Chamber and Rosfinmonitoring.

In course of the two-day workshop, the Rosfinmonitoring officers made the presentations.

The workshop attendees were mostly interested in the AML/CFT typology exercises, in particular:

- Methodological approaches used for conducting AML/CFT typology exercises: main aspects of macro-analysis of the precious metals and stones sector, transactions and their parties, suspicious transactions and deals criteria;
- ML and FT typologies: VAT evasion schemes; inter-bank "shadow" schemes used for cashing of funds, introduction of illegal gold into legal circulation and evasion of VAT; loans in precious metals or secured by precious metals.

Training for the staff of the Central Bank of Russia on Legal Regulation and Current AML/CFT System Development Trends

The Central Bank of Russia operates in the capacity of the macro-regulator of the financial market. Under Article 4 of the Federal Law on the Central Bank of the Russian Federation (Bank of Russia) it performs following supervisory functions:

- supervises operations of credit institutions and banking groups;
- regulates, monitors and supervises operations of non-credit financial institutions in compliance with the federal laws;
- supervises national payment system
- monitors and supervises compliance by securities issuers with the legislation of Russia on joint stock companies and securities;
- regulates, monitors and supervises corporate relationships within joint stock companies.

The International Training and Methodology Center for Financial Monitoring arranged two training events on important issues of legal regulation and current AML/CFT system development trends for the Bank of Russia personnel in charge of AML/CFT activities. Both events were held in Bank of Russia on the 21st and 23rd of October, 2014, respectively.

The purpose of these workshops was to raise awareness of the attendees about the main changes and modifications in the Russian AML/CFT legislation, clarify the FATF risk-based approach to payment systems and virtual currencies, inform about AML/CFT-related analytical researches and studies and present the outcomes of cooperation of banks with Rosfinmonitoring and coordination between Bank of Russia and Rosfinmonitoring.

In the course of the workshop, special attention was paid to Federal Law No.173-FZ dated 28.06.2014 on Specificities of Financial Transactions with Foreign Nationals and Legal Entities, on Amendments to the Code on Administrative Offences of Russia and on Invalidation of Certain Provisions of the Russian Federation Laws. The said Law came into effect on July 1, 2014 and made it possible to apply the provisions of the US Foreign

Pavel V. Livadny, State Secretary and Deputy Director of Rosfinmonitoring

Officers of the Federal Tax Service attending the workshop in the ITMCFM conference room, November 7, 2014

Account Tax Compliance Act in the territory of the Russian Federation.

The workshops were attended by 82 officers from various Departments of the Bank of Russia, including Financial Monitoring and Foreign Exchange Control Department, Security and Information Protection Department, Legal Department, Internal Audit Department, Statements Collection and Processing Department, National Payment System Department, Financial Markets Development Department, Insurance Market Department, Market Access Department, Securities and Commodities Markets Department, Microfinance and Financial Inclusion Department, etc.

The topics dedicated to AML/CFT analytical researches and the outcomes of cooperation between the Central Bank of Russia and Rosfinmonitoring attracted a special interest of the attendees.

AML/CFT Training for the Federal Tax Service Staff

On November 7, 2014, the ITMCFM hosted the AML/CFT training workshop for the officers of the Federal Tax Service.

During the session were elaborated issues pertaining to enforcement of the AML/CFT legislation of Russia; risk-based approach (the core element of the FATF standards); methodological approaches to AML/CFT macro-analytical and strategic researches; and ML/FT typologies.

Also were clarified the issues related to AML/CFT internal control arrangements, inspection/audit procedures, imposition of liability for non-compliance with the AML/CFT legislation of the Russian Federation, and ML schemes used in entities that operate betting shops, bookmaker offices, lotteries and other games of chance.

It should be noted that the most important research document on supervision of the betting sector is the FATF Report Money Laundering through the Football Sector. Misuse of the football sector for laundering criminal proceeds indicates that multiple flows of funds and wide range of financial transactions enhance the ML risk. It applies to ownership of football clubs, transfer market and ownership of football players, image rights, sponsorship and advertising agreements.

***

The training events held for the supervisors allowed the participants to share their views, opinions and best practices in a productive manner, to enhance the knowledge of the officers of the supervisory agencies and to strengthen inter-agency relationships and coordination in AML/CFT sphere.

It stands to mention that development and implementation of the training programs based on the comprehensive and updated domestic and foreign AML/CFT practices contributes to establishment of effective financial monitoring framework in the Russian Federation.

NEWS BLOCK

Regarding the Meeting of Council of CIS Foreign Affairs Ministers

On October 9–10, 2014 meetings of the Council of the CIS Heads of States and the Council of the CIS Foreign Ministers were held in Minsk, the capital of the Republic of Belarus that is chairing the Commonwealth of Independent States.

Significant attention was paid to security issues in the framework of the CIS. Participants approved the draft program of cooperation in combating illegal migration, the concept of cooperation in combating human trafficking. Meetings considered the extension of cooperation in strengthening of border security at external boundaries of the Commonwealth states, as well as collaboration among financial intelligence units.

Several international agreements and other documents related to the national security including the Protocol for Amendment of the Agreements of Establishment of the Council of Heads of Financial Intelligence Units of the CIS Member States were approved and signed by the presidents of the CIS member states.

The Protocol implies resolution of a number of organizational issues pertaining to activities of the Secretariat of the Council of FIU Heads whose functions – according to the resolution of the heads of financial intelligence units who signed the Protocol – have been performed by Rosfinmonitoring since June 2013.

During the events, the Federal Financial Monitoring Service was represented by the State Secretary – Deputy Director P.V. Livadny.

FATF Report: "Risk of terrorist abuse in non-profit organizations"

Terrorist organizations and non-profit organizations have different goals but to achieve them they often rely on similar resources. Money, materials, personnel, and social influence are key resources for non-profit organizations (NPO), but terrorist organizations are also trying to use them. That makes NPOs vulnerable to abuse by terrorists or terrorist networks.

The 40 Recommendations of the Financial Action Task Force (FATF) contain special provisions relating to non-profit organizations, which represent a valuable, albeit rather vulnerable sector. These provisions are included in Recommendation 8 (former Special Recommendation VIII), which states

that FATF members should take steps to combat the misuse of NPOs for the purpose of terrorist financing.

This typology report examines in detail how and where NPOs run the risk of being abused by terrorists. The report includes case studies and data from law enforcement and other government agencies, as well as from NPOs themselves, and is intended to raise awareness about the methods and risks of NPOs abuse for terrorist purposes both domestically and internationally.

The study answers the following key questions:

- Which NPOs are most at risk of abuse by terrorist organizations?
- What is the nature of the threat posed by terrorist organizations to the NPO sector?
- When are NPOs most at risk of abuse by terrorist organizations?
- Where are NPOs most at risk of abuse by terrorist organizations?
- Why are NPOs at risk of abuse by terrorist organizations?
- How
  - do NPOs become vulnerable to terrorist activities?
  - do terrorist organizations abuse NPOs?
  - is NPO abuse detected and suppressed?

The report stresses that NPOs are at risk of abuse for terrorist purposes at different levels: from the misappropriation of funds collected in the street to the penetration of terrorist organizations into aid programmes to promote their ideology.

There are also other factors that make the NPO sector very attractive to terrorist organizations, e.g. globalization, high employee turnover and high level of public trust.

The report provides an understanding of the risk of terrorist abuse in the key areas of NPO activities:

- collection of resources,
- storage of resources,
- transfer of resources,
- use of resources,
- implementation of programmes.

The typology report contains a number of indicators of NPO abuse or high risk of such abuse to help all stakeholders, including NPOs, government entities, financial institutions and designated non-financial businesses or professions (DNFBPs), identify and investigate possible cases of abuse involving separate non-profit organizations or the entire NPO sector.

FATF report "The role of HAWALA and other similar service providers in money laundering and terrorist financing"

Hawala and other similar service providers (HOSSPs) arrange for transfer and receipt of funds or equivalent value and settle through trade, cash, and net settlement over a long period of time. What makes them distinct from other money transmitters is their use of non-bank settlement methods.

This typology reviews three major types of HOSSPs defined by legitimacy or illegitimacy of their use and ML/FT risks connected with them.

- pure traditional (legitimate) ones;
- hybrid traditional (often unwitting) ones;
- criminal (complicit) ones.

There are several reasons why HOSSPs continue to pose a money laundering and terrorist financing vulnerability. These include:

- a lack of supervisory will or resources;
- settlement across multiple jurisdictions through value or cash outside of the banking system (in some cases);
- the use of businesses that are not regulated financial institutions;
- the use of net settlement and the commingling of licit and illicit proceeds.

While the settlement through value or trade that masks the individual funds transfers is a source of vulnerability, the most significant reason for concern is lack of supervisory resources and commitment to effective regulation.

FATF report "Financial Flows Linked to Afghan Opiates trafficking"

During the meetings of the FATF's Working Group on Typologies (currently the Risk, Trends and Methods Group) in Rome (June 2012) and in Paris (October 2012), the Russian Federation initiated a new typology research on this issue under the Strategic Surveillance Initiative.

The proposal received the support of several FATF member states (United Kingdom, India, Italy, Canada, China, Norway, USA, Switzerland and South Africa), three FATF-style regional bodies (the Asia-Pacific Group, the Eurasian Group and MONEYVAL) and two international organizations (the International Monetary Fund and the World Bank). The active phase of the research began in June of 2013.

The report aims to raise awareness about financial flows linked to Afghan opiates trafficking. Afghanistan is the world leader in the production and trafficking of opiates, with revenue from these illegal activities, according to some estimates, totaling $70 billion. Despite the efforts of the international community, the volume of Afghanistan's opium poppy production, at least in the southern provinces, remains very high – so high in fact that it broke a new record in 2013.

Little is known about the «business model» of the Afghan opiate trade. We know, for example, that on a global scale only a portion of drug-related funds and assets are seized, while the majority of revenue makes it safely into the legal financial system.

The report analyzes financial transactions linked to Afghan opiates trafficking. The data gathered show that the bulk of proceeds derived from opiates trafficking come to, are redistributed (typically through the use of money or value transfer services (MVTS)) and possibly even stored in the so-called financial centers. The report also identifies other methods used by drug traffickers to carry out transactions and distribute opiates.

Another conclusion is that the Afghan Taliban is actively involved in opiates trafficking. The growing trade in opiates will soon become one of the leading sources of income for the Taliban and may well provide the organization with enough funding to mount a credible threat to the national security of Afghanistan and the region as a whole.

The report and the case study are intended to assist in the detection of financial transactions involving opiates. They also provide financial centers with information about the factors that make them attractive and vulnerable to financial transactions involving the proceeds from drug trafficking and other crimes.

Translated FATF reports could be found on ITMCFM website.

Rosfinmonitoring held a board meeting

The Board meeting "Regarding the Progress of Establishment of the Performance (Efficiency) Assessment System and Regarding Improvement of Control System" was held in the Federal Financial Monitoring Service on December 3, 2014.

In his opening speech, Director of Rosfinmonitoring Yu.A. Chikhanchin pointed out that in the current international political and economic circumstances, risks and threats to the national anti-money laundering system rise sharply, both on international and national level: *"National leaders offer us tasks that make and bind us to revise our approaches and functional duties – clearly define objectives, roadmap, and anticipated outcome, to revise the planning system, to build a new mechanism of control and adoption of managerial solutions in order to ensure timely detection of arising problems and adjust our operations. In addition to our traditional tasks, we have to find our place in the developing system of state control – primarily, financial control. We should promptly detect emerging risks, threats, and – together with ministries and departments concerned – take all necessary measures to eliminate those."*

Among the key "expectations" from the national anti-money laundering system and from Rosfinmonitoring in particular, the following were emphasized during the meeting:

- compliance with international standards;
- encompassing all elements of the AML/CFT system in resolution of problems indicated;
- legal compliance of financial institutions;
- cooperation with control, supervisory authorities;
- measures to facilitate registration of criminal activities and criminal assets and return thereof to the owner;
- extinction of channels for financing of terrorism and weapons of mass destruction;
- implementation of amendments to relevant regulations aimed to enhance the anti-money laundering system.

"All the mentioned outcomes should be converted in definite figures, we should see dynamic of the events in progress, Yu.A. Chikhanchin said. *Efficiency of our activities should generally be reflected in prevention of "appropriation" – of budgetary funds, in the first place – and in decriminalization of economy and financial institutes. We must see that our approaches are sound and anti-money laundering activity is efficient."*

Research-to-Practice Conference "Current Problems of Combating Extremism and Terrorism"

Inter-departmental research-to-practice conference "Current Problems of Combating Extremism and Terrorism" was held on December 4, 2014 under the auspices of the All-Russian Advanced Training Institute of Employees of the MIA of Russia with the assistance of the International Inter-Departmental Center for Training and Re-Training of Specialists in the Sphere of Combating Terrorism and Extremism.

The conference was attended by more than 60 representatives of the Ministry of Internal Affairs, the Federal Security Service of Russia, the Federal Correctional Service of Russia, the General Prosecutor's Office of the Russian Federation, Rosfinmonitoring, the International Training and Methodology Center for Financial Monitoring, the Antiterrorist Center of the CIS Member States, employees of the Division for Combating Extremism of the Ministry of Internal Affairs of Russia as well as representatives of the Ministry of Internal Affairs, Principal Internal Affair Departments, Internal Affair Departments of constituents of the Russian Federation, lecturers and trainees of the All-Russian Institute of Advanced Training of Employees of the Ministry of Internal Affairs of Russia.

During the meeting, conference participants presented over 25 reports covering several important areas of anti-terrorism and extremism activities, among them are: combating terrorism under the current conditions; information warfare; new developments in the use of information networks by extremists and terrorists; interagency cooperation between government and law enforcement agencies in combating terrorism and extremism; topical issues of combating extremism and terrorism in the Northern Caucasus; challenges linked to the identification, detection and investigation of religiously motivated crimes committed by extremists; detection and suppression of terrorist financing channels, etc.

Representatives of financial intelligence units of Russia presented the following reports: "Current Provisions of Antiterrorist Legislation Pertaining to Freezing (Blocking) of Terrorists' and Extremists' Assets" (Ph.D. in Economics M.V. Kolinchenko, Rosfinmonitoring), "International Standards in the Sphere of Combating Financing of Terrorism" (E.V. Uskova, Rosfinmonitoring), "Current Problems of Illegal Abuse of Non-Profit Organizations for the Purposes of Money-Laundering and Financing of Terrorism, FATF International Practices" (N.A. Bobryshev, ITMCFM), "Education and Training in the Sphere of Anti-Money Laundering and Combating the Financing of Terrorism – New Trends" (Ph.D. in Education E.V. Ledyaeva, ITMCFM).

In acknowledgement of the importance and relevance of the organized event, participants of the research-to-practice conference extended their gratitude to the All-Russian Advanced Training Institute of Employees of the MIA of Russia for the opportunity granted by the latter to pursue joint discussion of current problems in combating extremism and terrorism. Publishing of the conference reports' digest is anticipated.

Publisher

I. V. Ivanova – editor –in- Chief, K. V. Litvinov – deputy Editor-in-Chief,
A. V. Pascal – editor-columnist, P. V. Kukushkin – editorial Coordinator,
I. A. Lisina – editor and correspondent, E. N. Kalikhova – editor-columnist,
E. V. Ledyaeva – columnist, A. V. Bulaeva – correspondent,
K. G. Sorokin – special correspondent, Y. V. Mazina – editor of the English issue.

Address: The International Training
and Methodology Center for Financial Monitoring
31, building 1, Staromonetny Lane,
Moscow, Russia, 119017. E-mail: info@mumcfm.ru.

Publisher: Autonomous Non-Profit
Organization ITMCFM.

Number of copies: 250.

Autonomous Non-Profit Organization ITMCFM

2014