FINANCIAL SECURITY

NO. 4 MARCH 2014

E.S. NABIULLINA:

Expulsion from the market place of those credit institutions whose customers carry out questionable transactions is of paramount importance for the recovery of the banking sector

FINANCIAL SECURITY

CONTENTS

EDITORIAL BOARD

Chairman of Editorial Board

Yu. A. Chikhanchin

Deputy Chairman of Editorial Board

V. V. Ovchinnikov

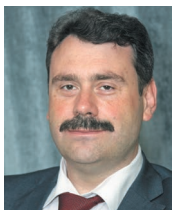
MEMBERS OF EDITORIAL BOARD

Yu. F. Korotky

G. V. Bobrysheva

V. I. Glotov

A. S. Klimenchenok



P. V. Livadny

V. P. Nechaev

A. G. Petrenko

A. N. Frolov

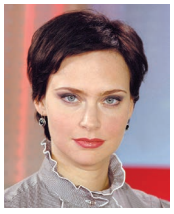
EDITORS

Editor-in-Chief

I. V. Ivanova

Deputy Editor-in-Chief

K. V. Litvinov



Editor-columnist

A. V. Pascal

Editorial Coordinator

P. V. Kukushkin

Editor and correspondent

I. A. Lisina

DEAR READERS!

Dear readers,

You are holding the latest issue of the *Financial Security* magazine, the first in 2014.

In his December 12, 2013 address to the Federal Assembly, the President of Russia outlined the key milestones of our work in 2014, setting a clear direction for the country's entire anti-money laundering system.

The unusual for the Russian language word «de-offshorization» has now firmly established its place in the vocabulary of economists, financiers, lawyers and other professionals. The underlying negative connotations for the Russian economy are significant, meaning that the phenomenon of offshorization, i.e. the use for business purposes of legal entities registered in countries with preferential tax treatment and/or a lax transaction disclosure regime, continues to receive increasing attention. The growing concerns over the high level of offshorization of the Russian economy is the logical conclusion drawn by the President in his address that determined the direction of our future movement. The policy toward de-offshorization of the Russian economy will be pursued both at the national and international level.

The task of reducing the level of the Russian economy's dependence on offshore is relevant to many areas of the Russian law and requires consideration of all identified reasons for using offshore jurisdictions, prompting a discussion of the topic by numerous agencies.

Rosfinmonitoring jointly with the Russian Ministry of Finance, Ministry of Economic Development, Ministry of Industry and Trade, Foreign Ministry, Ministry of Labor, the Ministry of Communications, Justice Ministry, General Prosecutor's Office, Federal Security Service, Interior Ministry, Federal Drug Control Service, Federal Tax Service, Federal Customs Service, Investigative Committee and the Bank of Russia have shown consistency in decision-making aimed at significant reduction in the level of the Russian economy's offshorization dependence. This work has culminated in the drafting of the National Action Plan to Combat Tax Evasion and Concealment of the Beneficial Owners of Companies, which was submitted to the Government of the Russian Federation for consideration.

However, we must realize that success in reducing the use of offshore companies in the economy depends not only on a competent public policy, but also requires a proper understanding of all the negative risks by the business community. The need for de-offshorization is obvious, while the relevance and effectiveness of the measures taken will depend on the quality of the dialogue not only between different agencies, but also with the private sector.

Rosfinmonitoring Director
Yury Chikhanchin

THE JOURNAL GUEST

AMONG THE MAIN CHALLENGES FACING THE BANK OF RUSSIA IS ENSURING EFFICIENCY AND EFFECTIVENESS OF BANKING SUPERVISION

Interview with the Chair of the Central Bank of the Russian Federation Elvira S. Nabiullina

Elvira S. Nabiullina

***FB:** How is the Bank of Russia getting on with its new job of a mega-regulator?*

E.N.: The board of directors of the Bank of Russia has voted to disband the Bank of Russia Financial Markets Service starting from March 3, 2014 and establish within the structure of its central office 9 new structural units responsible for the development and functioning of financial markets.

Let me remind you that the Bank of Russia Financial Markets Service itself was created within the structure of the Bank of Russia on September 1, 2013, taking over all of the responsibilities of the FFMS and some of the Finance Ministry for financial markets regulation, monitoring and oversight.

Among the entities that have been made accountable to the Bank of Russia are institutions that form the infrastructure of the financial market, as well as private pension funds, microfinance institutions, credit consumer cooperatives (including agricultural and housing savings), credit bureaus, rating agencies and pawnshops. The Bank of Russia has also been given powers to regulate, monitor

and oversee the activities of professional securities market participants.

The Bank of Russia has launched an initiative aimed at enhancing the role of self-regulation in the financial market characterized by rising participant numbers and worsening qualitative statistics. By improving self-regulation, we will be able to form a coherent regulatory system that will ensure an adequate level of control over the activities of market participants, as well as protecting the rights of consumers of financial services.

Improvements to the organizational structure of a single financial markets regulator will, on the other hand, allow the Bank of Russia to create for domestic financial institutions a modern regulatory environment, the quality of which will reflect the best international practice, and thus enhance the competitiveness of the domestic financial market and investment attractiveness of our country in the eyes of foreign investors.

FB: *What was the year 2013 like in terms of its influence on the country's banking system in general and the Bank of Russia in particular?*

E.N.: Despite a slowdown in the domestic economy, the growth in the Russian banking sector remained steady: its assets increased by 16.0% in 2013 to 57.4 trillion, mostly thanks to the expansion of lending.

Last year saw the banking sector come closer to the targets outlined in the Russian Banking Sector Development Strategy until 2015. Pursuant to this Strategy, the January 1, 2016 assets to GDP target is 90%, with non-financial institutions and individuals loans to GDP set at 55-60%. The actual figures for January 1, 2014 are: assets to GDP ratio reached 84.7 %; loans to GDP stood at 49.2%.

During 2013, the volume of loans granted to non-financial institutions increased by 12.7%. The future volume of lending to the non-financial sector will depend primarily on the state of the economy and the level of companies' demand for credit.

The adopted by the Bank of Russia regulatory decisions on assessment of consumer lending risks, coupled with the reassessment of risks by the banks themselves, have yielded results: the annual growth rate of loans to individuals is gradually slowing down, from 39.4% in early 2013 to 28.7% as of January 1, 2014).

The 2013 consolidated profit of credit institutions amounted to 993.6 billion rubles, which is slightly lower than in 2012. The main factors accounting for the decline are a more conservative estimate of the risks taken by banks and the creation of additional reserves to cover possible losses. The banking sector's own capital, on the other hand, increased last year by 15.6% to 7.1 trillion rubles.

Among the big factors influencing the future development of the Russian banking system are innovations in the area of banking regulation. In this context, in October 2013 Russia enacted Federal Law No. 146-FZ «On amendments to certain legislative acts of the Russian Federation». The new law is designed to introduce into the Russian banking practice the internationally recognized approaches to banking regulation and oversight, including those recommended by the Basel Committee on Banking Supervision.

The entry into force of this law creates the conditions for application by credit institutions for regulatory purposes of the approaches based on internal ratings to determine the capital requirements and to enforce the «Supervisory Review» (Pillar 2) and «Market Discipline» (Pillar 3) concepts of Basel II. At the same time, the Bank of Russia has been given the powers to assess the quality of internal models used by credit institutions for assessment of their capital requirements, and to establish risk and capital management standards for credit institutions and banking groups, as well as banking requirements for the development and implementation of the internal capital adequacy assessment procedures, etc.

The adoption of the law No. 146 -FZ has significantly improved the quality of consolidated supervision by clarifying the term «Banking Group» in terms of inclusion into it of all entities, irrespective of their line of business, under the control or significant influence of a single credit institution, as well as expanding the powers of the Bank of Russia in respect of bank holding companies.

Of particular importance is the fact that this law has granted the Bank of Russia the authority, starting from January 1, 2015, to exercise professional (motivated) judgment regarding the existence of any connection between a credit institution and legal and natural persons, and to establish a new mandatory requirement limiting the risks that can be taken on by credit institutions from transactions with these persons.

In general, we can say that, starting from 1 January 2014, the Bank of Russia has been implementing the key concepts of Basel III (including in terms of determining capital adequacy and its components) in its supervisory practice.

***FB:** Still, some problems remain: capital flight, illegal cash-out transactions, etc. How does the Bank of Russia react to these challenges and threats?*

***E.N.:** :* Indeed, for quite a long time one of the weaknesses of the Russian banking sector was associated with the high level of involvement of certain credit institutions in the provision of services to customers who carry out so-called «questionable» transactions.

There are two main problems here.

The first one is connected with the siphoning off capital abroad on questionable grounds. In 2012, its volume totaled $39 billion and about $22 billion in the first 9 months of 2013. To do this, some unscrupulous businesses have been actively using in recent years the opportunities linked to the measures designed to facilitate the movement of goods within the Customs Union. According to our estimates, about 48 billion dollars was taken out of the Russian Federation in 2012-2013 using such schemes.

The second problem is connected with illegal cash-out transactions, valued at hundreds of billions of rubles per year.

To counter these challenges, the Bank of Russia has expanded the banks' mandate for tracking suspicious transactions of their customers.

Today banks have the authority to:

1) refuse to a open a bank account in a wide range of situations where it is suspected that such account (deposit) can be used for money laundering and terrorist financing purposes;

2) refuse a client's order to execute a transaction, except for deposit transaction;

3) terminate a contract of bank account (deposit) with a client in the event of two or more bank refusals during a calendar year to execute the client's transactions.

***FB:** How do think the future work on «cleansing» the system of criminal and unscrupulous transactions should proceed?*

E.N.: Expulsion from the market place of those credit institutions whose customers carry out questionable transactions is of paramount importance for the recovery of the banking sector.

This work has brought about a decline in suspicious money siphoning transactions carried out by clients. For example, the number of such transactions went down 16% in Q3 2013 vs. Q2, with the number of such transaction in the segment of foreign trade within the Customs Union declining by more than 40%. According to preliminary estimates, this trend was also continued in Q4. Most credit institutions respond adequately to the measures taken by the regulator and use the opportunities provided by law. A survey conducted by the Bank of Russia shows that in the 3rd quarter of last year a total of 54 credit institutions stopped executing suspicious customer transactions.

However, in respect of certain credit institutions, the Bank of Russia has no choice but to take more stringent measures based on the entire body of evidence available to it. Unfortunately, we must admit that we do not always have enough power to deal with such credit institutions. For this reason, the Bank of Russia, together with the relevant ministries and agencies, is working to modify legislation in this area and extend a set of legislative tools needed to deal with questionable transactions.

***FB:** How would you evaluate the level of the banking system resistance to risks?*

***E.N.:** :* In order to assess the level of financial system risks, we use a wide range of analytical tools, including «risk maps», financial stability indicators and quarterly stress tests of the Russian banking sector.

For example, the stress test conducted on October 1, 2013 was based on two scenarios whose characteristics were determined based on the estimates of the possible impact on the Russian economy of the worsening global economic outlook. The scenarios under review differ in terms the magnitude of the specified shocks and reflect the exceptional, yet probable developments.

The results of the current stress tests generally fall within the range of estimates obtained in the course of stress tests performed in 2008-2012. For this reason, the Bank of Russia generally considers the stability of the banking sector as adequate in relation to the current state of the economy and foreign economic conditions. That said, possible risks associated with the banking sector and individual banks are constantly in the spotlight, meaning that appropriate regulatory and supervisory measures can be taken whenever needed.

FB: *In 2013, Russia enacted the 134th Federal law No. 134-FZ, giving banks, regulators, supervisors and law enforcement agencies new tools with which to tackle illegal financial transactions. All this requires some restructuring of banks' operations. How is this process going?*

E.N.: The mission of the Bank of Russia relating to the enforcement of this law lies in using the existing supervisory tools to encourage credit institutions and other supervised entities to use the new powers granted by the 134-FZ. That said, the focus is placed on the proper use of these powers, rather than on formal actions. This challenge requires financial institutions to restructure their internal money laundering procedures and place greater emphasis on the so-called «risk-based approaches».

The information available to the Bank of Russia allows us at this stage to say that the banking system as a whole has reacted positively to the new tools and begun actively using them in practice.

FB: *What are the challenges facing the Bank of Russia in the near future, including in terms of its interaction with Rosfinmonitoring?*

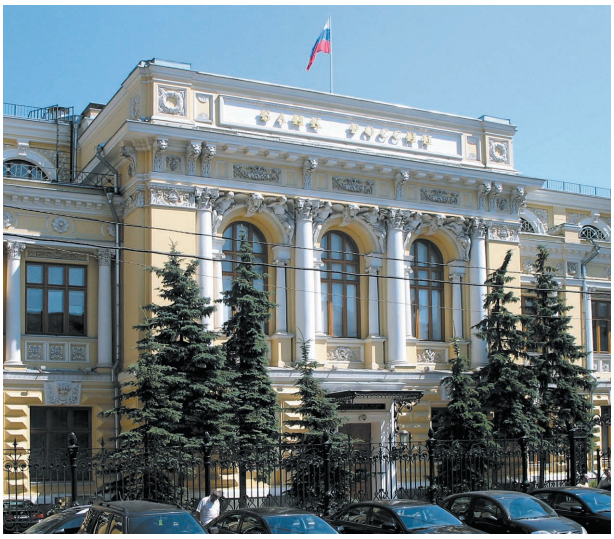
E.N.: Among the main challenges facing the Bank of Russia in the near future is, above all, ensuring efficiency and effectiveness of banking supervision.

In pursuance of its banking sector recovery policy, the Bank of Russia assesses the transparency of credit institutions, as well as the quality of their management, assets and capital. When necessary, banks may be required to restore stability or undergo measures aimed at limiting additional risks they may take on.

If there is no realistic prospect of future financial stability, the bank's license is revoked, or the bank undergoes restructuring. When taking a decision about restructuring, the issue of economic feasibility plays a key role, as do the systemic effects of license revocation.

Improving the level of credit institutions' reporting credibility and accuracy is one of the Bank of Russia's main priorities. To achieve this goal, we will need, among others, some legislative changes that will allow, for example, the banking regulatory authority to permit adjustments to be made to reporting statements (including in the cases of bank assets and capital overstatement or recording of transactions with short-lived companies, including of questionable character).

Another effective measure would be to introduce criminal liability for concealment in reporting documents of signs of bankruptcy or grounds for license revocation.



For its part, the Bank of Russia will continue to improve the regulatory framework governing the banking sector. In particular, the Bank of Russia plans to adopt regulations establishing the procedure for identifying person (persons) possibly connected to a credit institution and specifying the actions to be taken by the Bank of Russia's structural units overseeing the activities of credit institutions to identify individuals who can be classified as persons related to a credit institution.

With regard to the joint work with Rosfinmonitoring, our short-term AML/CFT goal here is, in our opinion, to do all we can to help credit institutions integrate the mechanisms provided for in the updated legislation into their work, dispose of customers carrying out questionable and money laundering transactions and suppress their activities.

We also hope that the use by credit institutions of risk-based approaches based on the new international standards, especially the FATF Recommendations, will strengthen the reputation of the Russian banking and financial markets.

FB: *The Bank of Russia has initiated amendments to the school curricula in order to improve financial literacy. Is it necessary? And what exactly does «financial literacy» mean in relation to an average person?*

E.N.: Financial literacy is an important condition for protecting legitimate rights and interests of our citizens in the world of finance.

The Bank of Russia plays an active role in this educational work. For example, we have prepared a series of lectures for pupils, students, middle-aged people and pensioners that are going to be held in the halls of the Bank of Russia's museum and exhibition center. Also, we plan to launch relevant television and radio programs. The work on the «Financial Literacy» section of the Bank of Russia's website is almost finished. We intend to use it to educate kids and students of junior and middle classes by posting fairytales and visual information related to the topic of finance.

We are convinced that our financial literacy campaign is particularly relevant for young people, because it teaches them how to navigate through a variety of financial products and services that are offered on the market today and helps impart literacy skills needed to manage their finances effectively.

Teaching the basics of financial literacy to high school students could be one of the most effective mechanisms for improving financial literacy of the public. The Bank of Russia has initiated the establishment of a working group tasked with creating a financial literacy teaching kit (a textbook, a teaching guide and a CD with additional material) for high school students.

Currently, this working group is completing its work on a teaching kit on the basics of financial literacy for grade 9 secondary schools students, which will be launched soon. As this subject is new to the secondary school curriculum, its success will first be tested in several schools as part of a pilot project.

In general, dependence of the quality of people's lives on their financial knowledge is growing. The more people understand the opportunities presented by pension savings, wireless payments, etc, the greater the public confidence in the relevant segments of the country's financial market is, the faster they will grow and accumulate funds, thereby creating an investment resource for the development of the whole economy. The fewer, by the way, there will be opportunities for illegal activities of individual financial institutions, which is something not only the Bank of Russia, but also all law-abiding domestic financial market participants are interested in.

COVER STORY

COMMON GOAL IS TO KEEP CONFIDENCE OF THE RUSSIAN CITIZENS IN BANKING SYSTEM

The Conference dedicated to the vital issues of the government AML/CFT policy was held in Moscow on December 18, 2013. The Conference was initiated and arranged jointly by the Central Bank of Russia, Association of the Russian Banks and Rosfinmonitoring. Taking part in the Conference were the heads of the national law enforcement agencies, the officials of the Federal Tax Service, the representatives of the State Duma of the Russian Federation and the senior managers of some major financial institutions

Konstantin V. Litvinov,
Deputy Chief Editor

In his welcoming speech, **Mr. Garegin A. Tosunyan, the President of the Association of the Russian Banks**, stressed the importance of effective and targeted measures to be taken with the support of the law enforcement agencies for fighting criminals and fraudsters:

– Complete confidence in the banking system is the important element of immunity which allows the system to become more mature and gives the chance for further economic development. We need to undertake further efforts for exterminating the criminal and disreputable occurrences in the system, but at the same time it is necessary to minimize the negative impacts on the society, economy and business, since any struggle and therapy have the side effects. Success depends, to a large extent, not just on the regulators but also on our colleagues from the law enforcement agencies because it is important for the entire society that the efforts aimed at curbing all types of crooks and fraudsters are implemented efficiently and do not affect the bona fide and law-abiding citizens. This should be done not by treating all those who work in the commercial or banking sector as being presumed guilty, but by imposing tough sanctions against those who are brazenly and defiantly involved in criminal activities being convinced that they will pay

off the authorities to avoid prosecution in any case. I hope that we may reckon upon our law enforcement agencies and legislators since only by joining our efforts we can overcome this problem.

In her presentation, **Mrs. Elvira S. Nabiullina, the Chair of the Central Bank of the Russian Federation,** focused on the development of the national banking system in 2013 and denied all allegations of instability of the system:

– Recently, the so-called "black lists" have appeared and rumors about problems in certain banks have been circulated. I hereby reiterate that this is false information. We indeed withdraw the banking licenses, but it is the compulsory and necessary part of the work of the regulator in any country across the globe. Decisions to withdraw licenses, being the measure of last resort implemented as part of the supervision and regulation process, are taken only in compliance with the law on case-by-case basis. This helps to improve the market discipline and to enhance stability of the banking sector in general.

I hope that the AML/CFT measures undertaken by the Bank of Russia and the Russian banking community would strengthen the confidence within the banking system and also enhance the confidence of the government and, most importantly, of the customers in the banking system. Customers' confidence in the banking system and in its reliability and transparency is our priority and the main asset. This will help us to ensure that the national banking system meets the needs of the economic and social development of our country and also bring it in line with best international practices.

Mrs. Nabiullina presented some statistics supporting the stable development of the banking system in 2013. Eight banking licenses were withdrawn for breaching the Anti-Money Laundering Law, and another 54 banks terminated all shady transactions following their monitoring by the macro regulator, which is the clear evidence of their adequate response to the undertaken measures. According the Chair of the Central Bank the banking sector enjoyed the growth in terms of all basic indicators, such as the amount of assets, loans and deposits, in 2013. As of December 1, 2013, the assets growth rate reached 18%, the amount of loans granted to nonfinancial entities grew by 14.3%, and the increase in household deposits was 21%.

Mrs. Irina Y. Yarovaya, the Chair of the State Duma Committee for Security and Ant-Corruption, pointed out the importance of both political will and availability of the social institutions for addressing any issues and problems:

– I think that currently no one has doubts that the political will is strong enough for protecting not just the national economic interests, but also the interests of the Russian Federation citizens in the territory of our country against the so-called mala fide banks, that still emerge and in respect of which the Central Bank implements, in our opinion, absolutely adequate and lawful measures for deterring and terminating their illegal operations. We consider this as the targeted response, since any offence is committed by particular person(s) and is not of a general nature.

In this context, we pay special attention to the social institutions and to the role of the self-regulatory bodies. I think that the maturity of our national banking community allows us not to silently observe the operations of certain banks that are not fully in line with the law, but to raise the issues of their liability, since confidence and lack of confidence are two sides of the same coin. However, confidence takes long time and serious effort to be built. And given that currently the Russian Federation citizens have confidence in the banking system (which is proved by the increase in the household deposits), our common goal is to preserve and maintain this confidence by excluding possibility of abuse of the banking system.

After the announced presentations have been made, Mr. Yuri I. Kormosh, the Vice-President of the Association of the Russian Banks who acted as the Conference moderator, once again emphasized the importance of strict compliance by everyone with Federal Law No.134 for further improvement and enhancement of the banking system.

Presentation by Mr. Yury A. Chikhanchin, Director of Rosfinmonitoring

"Know You Customer" as the Underlying Principle of Operation of Credit Institutions for Decriminalization of the Economy

Good afternoon to all attendees to the Conference. We gathered here today to summarize the results of the outgoing year which has become the milestone for both the banking community and the government authorities involved in monitoring and supervision of credit institutions and the AML system, in general.

First of all, the Bank of Russia, being the national macro regulator, has become the fully-fledged and operational authority, which supervisory and regulatory responsibilities now cover not just the traditional but also new sectors of the economy, such as the securities market, micro-financing organizations, consumers credit unions, insurance sector, non-government pension funds and under-regulated electronic payments market.

It means that the high banking supervisory standards are extended to these sectors, which will definitely facilitate the efforts aimed at ridding them of the so-called "grey" technologies, and at the same time will improve the capabilities of the entities operating in these sectors by improving quality of the financial services, which will probably create the healthy competitive environment for banks, in general.

Secondly, the adopted Federal Law No.134 vested new powers in the regulatory banks, supervisors and law enforcement agencies enabling them to more effectively curb illegal financial transactions. This undoubtedly presents certain challenges to both the banking sector and the government authorities requiring them to restructure, to a certain extent, the style and methods of their work in the current situation where enhancement of transparency of the global and national economies and their de-offshorization and de-criminalization are the priorities set in the G8 and G20 agendas.

In his address delivered on December 12, 2013, RF President Vladimir Putin once again stressed that these objectives are still the priorities for Russia. However, thorough analysis of the decisions taken in 2013 clearly shows that despite emergence of new tactical objectives the strategic goals of the

banking sector related to prevention of misuse of the economic system remain the same and are based on two underlying principles: know your customer and manage risks for their minimization. In fact, banks are now entitled to refuse to execute customers' instructions if they suspect that transactions are related to money laundering or terrorist financing and may also terminate agreements with suspicious customers.

These are the powerful tools which, if used properly, can completely prevent infiltration of potentially criminal capital into the economy. But in the past, banks also worked with their customers, identified persons with whom they had business relationships, maintained customer files and terminated business relationships with customers when it was necessary. In the context of the new rights granted to banks, it is worth mentioning some innovations introduced by Federal Law No.134, namely: the obligations of credit institutions to scrutinize their customers, establish the purposes of business relationships with potential and existing customers and identify beneficiaries. I think that only through the practical application of these measures the revolutionary decisions under Federal Law No.134 can be implemented.

I believe that in such situation banks should implement the proactive customer outreach programs by constantly raising their awareness in compliance with the "know your customer" principle. In many cases it will help to avoid imposition of sanctions against customers, since not everyone who carries out dubious transactions is necessarily involved in

laundering of criminal proceeds or in financing of terrorism. Such customers may just need to receive a qualified assistance from a credit institution. By saying this I mean that banks should exercise caution and discretion in each case they terminate agreement with a customer and I am certain that they do it. Such approach, among other things, will allow to avoid two identified risks that currency arise as a result of unreasonable imposition of the sanctions, namely: the risk that funds of dubious customers will flow into the under-regulated sectors, and the risk of possible corruption of bank officers.

Thus, the intention of the developers of Federal Law No.134 that vests new powers in banks is not to force banks to automatically reject dubious customers, but to ensure that credit institutions continuously monitor their customers' operations and promote, if you will, the high economic activity standards among the customers. And credit institutions are the main and indispensible assistants of the Bank of Russia and Rosfinmonitoring in pursuing this goal. Another aim of the said Law it to raise the general financial awareness of the population and to prevent involvement of individuals into financial fraud schemes. The losses inflicted by such illegal activities amount to dozens of billions of rubles that are not paid to the budget and, therefore, cannot be invested in the development of the national economy. Prevention and fighting against such illegal financial transactions is the goal that should be pursued not only by the government but by the population as well.

At the same time, the business community should develop the new way of thinking and new style of doing business by clearly understanding and strictly complying with the following principle – Learn to Do Business without Theft. In this context, I would like to once again support the initiative of the Bank of Russia that proposed to the government to include the financial awareness raising subject in the high school educational program. This was also the main reason for establishing the Network Institute set up as the community of the leading higher education institutions in Moscow and in the Federal Districts which will develop common approaches, methodologies and training programs for AML compliance officers working in both private sector and government authorities.

I would also like to say few words about the measures undertaken by the Bank of Russia to rehabilitate the banking system. Liquidation of ailing entities that operate in the banking sector is the routine practice of the regulator. The Bank of Russia has done it in the past and will do it in the future, where necessary. If "Know Your Customer" is the motto of banks, the regulator's motto is "Know Your Supervised Sector". I would like just to point out that the measures implemented by the Bank of Russia in respect of credit institutions are the result of the efforts undertaken by all authorities engaged in the AML activities and by bona fide commercial banks that inform Rosfinmonitoring about their mala fide colleagues. These coordinated efforts are undertaken by the financial intelligent agencies that detect banks involved in money laundering, the law enforcement agencies that curb criminal activities of managers of non-credit institutions and the parliament that develops and adopts the laws for identifying and curbing money laundering mechanisms.

In his address, President Putin stated: "We need to maintain our fundamental firm position on ridding our credit and financial system of various types of money laundering entities and operations. Meanwhile, the interests of bona fide customers and depositors in problematic banks should be securely protected". Enhancement of transparency of the economy and decriminalization of financial transactions is not the one-time action involving application of several dozens of new legislative mechanisms, but the continuous efforts that include in-depth scrutiny of customers, analysis of activities and relationships of customers and identification of possible beneficiaries.

In the end of my presentation, I would like to remind that the adoption of the Russian report by the FATF Plenary last October confirmed that the national AML legislative framework had been brought in compliance with the international standards. In course of the on-site mission in 2015, we will need to convince the FATF experts in effectiveness of our anti-money laundering system.

PRIVATE SECTOR

PROBLEMS OF IDENTIFICATION OF E-PAYMENT TOOL USERS

Valery Lopatin,
Deputy Head of International Payment Department of Payment Service Directorate of State Corporation "Bank for Development and Foreign Economic Affairs (Vnesheconombank)"

E-payment tool (the «EPT») is a relatively new term[1], which appeared in the Russian law in 2011 when the Federal Law of June 27, 2011 No. 161-FZ «On National Payment System» (the «NPS Law») entered into effect.

According to the NPS Law, the EPT is a tool and/or a method enabling a client of a funds transfer operator (the «FTO») to draft, to certify and to send orders to transfer funds within the used cashless payment systems using IT and telecom tools, electronic media, including payment cards, and other technologies.

Legalization of the EPT drives their broad spreading and using by economic entities; at the same time, the unique consumer properties of the EPT promote the following:

- Significant enhancement of availability of payment services. Any EPT user may have access to payment services in 24/7 mode anywhere within the Russian territory;
- Streamlining the use of financial resources resulting from enhancement of availability of payment services and operation of information and analytic service integrated into the EPT;

[1] Officially, «E-Payment Tool» as a term appeared in 1996 in the Russian Civil Code (Part 2, Section 847) without any definition. Its context allowed for interpreting it as a document certifying the right to dispose money.

- Growth of the Russian economics. The last idea can be easily justified by the growth of the level of automation of payments (and related) transactions resulting in significant increase of productivity in payment industry and related market segments.

However, the same consumer properties of the EPT causes a number of problems related to EPT use increasing significantly the risk of its applying for criminal purposes, including money-laundering and terrorism financing. This article discusses a number of problem issues related to identification of EPT users, including identification and recognition of e-payment tools, identification of legal users, management of the risk of unauthorized transfer of ESP ownership and operation rights.

Identification (in the wide sense) means establishment of sameness of an unknown object/subject and a known one on the basis of matching features. Examples:

- Establishment of sameness of an unknown object and a known one on the basis of matching names, IDs and creation dates;
- Establishment of sameness of an unknown object and a known one on the basis of matching finger dermal ridges, etc.

Identification in the wide sense should be distinguished from identification in the restricted sense. The last term means allocation of an identifier to an object/subject and/or comparison of an identifier with the list of allocated identifiers.

Authentication means the procedure of verification of authenticity of an object/subject. This is mostly an IT term. Examples:

- Verification of authenticity of a user by compating the entered password with that stored in the data base of users;
- Verification of authenticity of an e-mail by comparing the hash function value of the received letter with that of the sent letter (on the basis of decoding the digital signature of the letter), etc.

Features of e-payment tools

Под определение ЭСП подпадает целый ряд The EPT definition covers a number of engineering solutions used to any extent for drafting, certification and sending the orders «for the purpose of funds transfer». First of all, they include electronic, web and mobile banking systems that have special payment functions as a rule. Moreover, traditionally the EPT include payment cards since they are directly referred to in the definition of the EPT. It is necessary to note that the payment cards cannot be used directly for drafting and sending payment orders. Therefore, in such case the EPT should include the payment cards operating with other devices: ATMs, POS terminals, etc.

The remote mode of drafting, certification and sending orders (when the user is beyond the office of the FTO) is a significant feature of all EPT. He/she can seat at dozens, hundreds and even thousands of miles away from the office without any personal contact with an officer of the FTO communicating by phone, visual communication channel or messaging. However, in general, such communication tools are used for managing incidents only, since they slow down and raise the cost of the payment process to a great extent.

Operational efficiency of drafting, certification and sending orders resulted from 24/7 availability of e-payment tools (subject to limitation of the use of EPT by organizations) and high level of automation of transactions. Surely, anything but all FTOs always accepts and processes funds transfer orders in 24/7 mode. However, there is a great payment segment (including payments within card systems and large e-money systems) enabling transfer of funds among EPT users separated by thousands of miles in 24/7 mode virtually at the same instant.

According to the definition, the users of EPT are customers of FTOs (individuals, organizations and sole proprietors). The customers use e-payment tools under Section 9 of the NPS Law on the basis of agreements on the use of EPT executed by FTOs with customers and between each other. At the same time, the NPS Law does not provide for any limitations

for modes and procedures of execution of such agreements. Therefore, e-money operators as FTOs execute a large number of customer agreements on the use of non-personalized EPTs under contracts of adhesion. In such case, a customer may accept FTO public offer by clicking at YES icon on a page of web browser or mobile application.

Identification of EPT and EPT user

In general, the object identification means a procedure of establishment of sameness of an unknown object and a known one on the basis of matching features (identifiers). Therefore, identification is based on development of the relevant set of identifiers and the procedure schedule, but they can differ much due to a number of circumstances, e.g.:

- Type of objects to be identified. In particular, identifiers of such EPT as payment cards and mobile phones with installed mobile application can be rather different.

- Required accuracy of identification. Usually, higher level of seriousness of negative effect of incorrect identification requires increase in accuracy of identification procedure. It is evident that any identification has its own accuracy. For instance, the identification based on three object identifiers is pretty certain more accurate than that based on one identifier.

- Required speed of identification. The period of time allocated for identification often limits availability of identification techniques. At the same time, the following rule is used in general: higher identification speed requires more strict limitations for identification accuracy.

More than one identifier are used for EPT identification as a rule. For example, the card number, the validity date, the cardholder name and CVV2/CVC2 code will be used mostly for identification of the payment card. As for hardware-software systems (the «HSS») wired to network (such as electronic banking systems), they can be identified by MAC (Media Access Control) unique identifier assigned to each active network device or by IP address (Internet Protocol Address) issued to each web node[2].

The case of web banking systems is somewhat more difficult, since integration of the identifier into HSS of the EPT user does not allow for using any PC anywhere within the network for accessing the payment services. In this case, identification of EPT as a device and/or software at the customer side is virtually unavailable, but it is compensated by increase in strictness of requirements to EPT identifier.

Good identification functionalities are demonstrated by mobile banking systems, since a mobile device has a set of features that can be used as EPT identifiers. In general, they include: IMEI (International Mobile Equipment Identity) code, the subscriber number, the identifier of installed OS version, etc.

As for identification speed, in the most cases FTO can use the whole period of communication between the customer EPT and hardware/software assets of FTO[3]. Moreover, FTO may enforce the lower threshold of communication period subject to selected accuracy and duration of EPT identification. However, this threshold should be sufficiently low - if not, the user can reject to use the EPT due to too long duration of transaction processing.

There are three types of identification of the user of EPT to be discussed:

- Based on identification of EPT assumed to be in hands of its lawful owner;

- Based on identifiers of the lawful EPT owner (recorded by FTO on execution of the contract with the customer/owner), assuming that the owner is the EPT user;

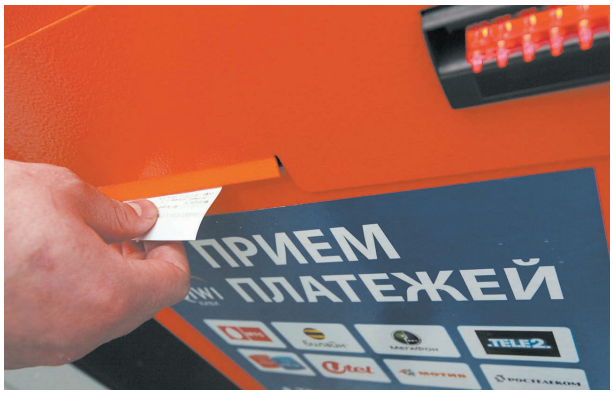
- Identification of the lawful EPT owner under the Federal Law of August 07, 2001 No. 115-FZ «On countermeasures against money-laundering and financing of terrorism» (the «ML/FT Law»), assuming that such owner is the EPT user.

There are a number of methods of identification of the EPT user based on his/her physical features, as well as on providing data remembered by the user. The first group includes fingerprint and iris-based identification

[2] A unique cookie identifier sent to the computer on its first connection with the bank and stored in computer memory can be used to identify the computer in the Web. If the computer user deletes the cookie file, the new cookie identifier will be issued on the next connection.

[3] If the EPT fails to pass identification, FTO may reject to accept and execute the customer order, even if the customer have managed to send it.

techniques as the most popular ones. The second group uses various PIN codes, logins and passwords to be memorized by the EPT user, as well as other data for password recovery and/or on security incidents.



Identification under the ML/FT Law provides for the complex of measures aimed at identification of certain information on customers, their representatives and beneficiaries, as well as verification of such information using original and/or duly certified copies of documents under ML/FT Law. FTO applies such identification procedure to all customers holding bank accounts, as well as to customers holding electronic accounts receiving corporate or individual e-payment tools (the «CEPT» or «IEPT» as appropriate). Results of identification of each customer are documented as a customer questionnaire to be updater on the regular basis and used by FTO under ML/FT Law.

Identification under ML/FT Law is performed as the first operation in the process of executing IEPT[4] and CEPT agreements or earlier in the process of establishing a bank account. Moreover, identification and authentication of the EPT user is performed at the beginning of each communication session of EPT and FTO HSS, then EPT and FTO HSS begin data exchange, which can include EPT identification, if available.

Problems of identification of ESP user

Refer to Fig. 1 for EPT operation flow diagram. The following problems exist within this technology due to EPT user identification features:

- Accuracy of EPT identification based on EPT identifiers agreed on execution of EPT agreement;
- Accuracy of EPT user identification based on EPT user identifiers agreed on execution of EPT agreement;
- Verification of assumption that EPT is in hands of EPT user set out in EPT agreement;
- Verification of information on EPT user provided during identification under ML/FT Law.

The problem of accuracy of identification of EPT on the basis of EPT identifiers agreed on executing EPT agreement relates to difficulties in revealing fake (copied) EPT. Modern IT systems allows for easy identification of EPT identifiers, comparison of them with pre-set identifiers and making decision on their matching. However, such systems can distinguish an original from its copy, only if at least one EPT identifier has been copied incorrectly. If the copy is good, FTO HSS determines that identifiers are valid, and EPT passes identification.

This problem can be solved by increasing the number of EPT identifiers and the level of complexity of copying, including the use of integrated microprocessor chips and complex algorithms of communication between EPT and FTO HSS. However, sufficient increase of complexity and the number of identifiers will lower identification speed that can be inappropriate concerning the consumer features of EPT.

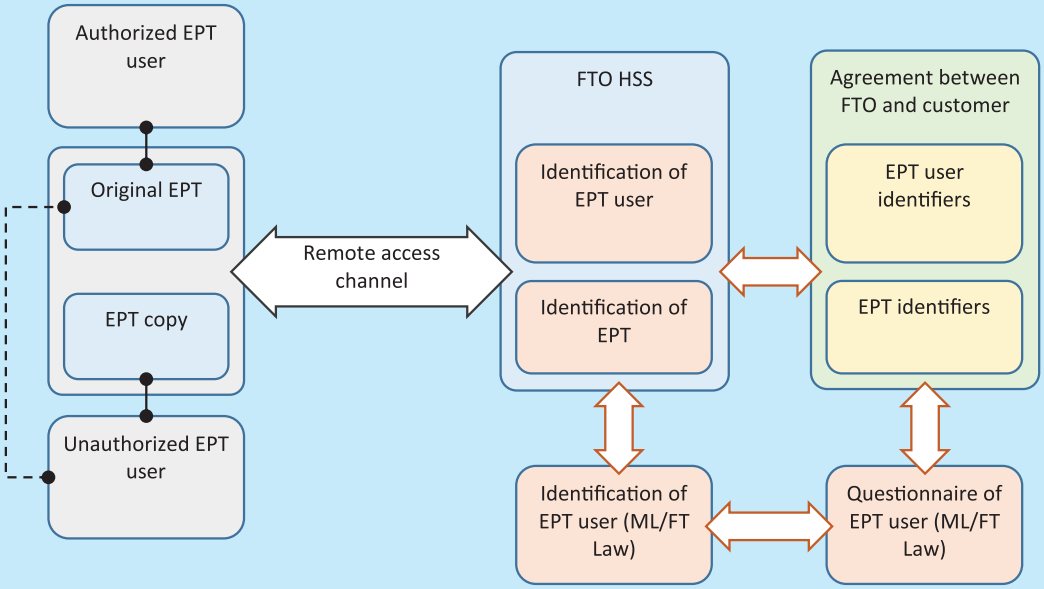
The problem of accuracy of identification of EPT user on the basis of EPT user identifiers agreed on executing EPT agreement also relates to difficulties in revealing fake (copied) user.

In many cases, the special authentication procedures based on requesting data sent to the user previously by secure channels can be helpful in revealing the unauthorized user. Therefore, identification of EPT users should provided for prior delivery of data from FTO to EPT user to be memorized and used for identification purposes by the user.

It should be noted that nearly always the problem of EPT copy is connected to fake user problem. Therefore, the identification methods able to solve both problems simultaneously can be used. In particular, digital chips integrating electronic signature tool can be used in EPT to solve this problem. Content of such chips is well protected against copying providing for easy revealing EPT copy used by an unauthorized

[4] Financial Monitoring and Foreign Exchange Control Department of the Bank of Russia informed that simplified identification may not be used on issuing IEPT, answering to the request of National Payment Council Non-Commercial Partnership (letter of 20.09.2013 No. 12-1-5/1514).

Fig. 1: Interaction process during the use of EPT



user. However, this method fails, if an unauthorized user uses original EPT.

Therefore, verification of possession of ESP by an authorized user (specified in EPT agreement) is the central problem of identification. As discussed above, this problem can be solved partially by identification of EPT user by authentication procedures. However, criminal transaction can be performed by unauthorized users with original EPT.

It is evident, that assessment of reliability of assumption that EPT is in hands of the authorized user has probabilistic nature. Therefore, the risk of unauthorized use of EPT determined as combination of results of the unauthorized use and probability of such results can be used as a probabilistic feature[5].

The level of risk can be assessed by various methods developed for risk management processes. In particular, they can include methods of processing statistic data on EPT location in the network, nature of its previous use, etc. For example, lowering of reliability of data on possession of a payment card by its authorized user can be a result of changing a country of card transaction, increase of amounts and frequency of transactions, etc.

The problem of verification of information on EPT user provided during identification under ML/FT Law does not relates to such users, therefore, it is not discussed here in details. However, it is necessary to note that the data from the customer questionnaire can be used for assessment of the risk of the unauthorized use of EPT. Therefore, they can influence much the assessment of reliability of assumption that EPT is in hands of the authorized user.

[5] ISO 31000:2009 «Risk Management - Principles and Operation».

FINANCIAL MONITORING OF AGENCY NETWORKS: CHALLENGES AND SOLUTIONS

Dmitry P. Gronin,
Head of Financial Monitoring Department, Platina Bank

Nadezhda V. Sorokina,
Principal Economist of Financial Monitoring Department, Platina Bank

The agency arrangements in the national payment systems are becoming more and more widespread. The agency networks are advantageous since they ensure broad financial inclusion, provide for extended access to financial services for end-users (customers) and allow for making low-value payments. Besides that, they give small businesses the opportunity to relatively easily enter the market due to simplified supervision procedures and lack of any licensing and additional registration requirements. Typically, a payment agent is subject to monitoring by the principal who takes the risks related to quality and nature of agency transactions.

In Russia, the agency arrangements for provision of financial services are featured by "dual" regulation. The right to render the intermediary services involving acceptance of payments for the benefit of third parties arises either under a sub-agency agreement with a payment operator that has direct agency

agreements with providers of goods and services, or under an agency agreement with a credit institution through which payments are made to providers of goods and services under the Law on Bank and Banking Activities.

Monitoring of agents that directly accept payments from individuals and provide money transfer services is complicated not only by the dual nature of the regulation, but also by two types of entities that are subject to monitoring (the money transfer operators and the payment acceptance operators) and by the fact that the government supervision is performed by two agencies (the RF Central Bank and Rosfinmonitoring). The variety of the types of agency

networks as well as the desire of the legislators to make these services more convenient for the users quite often create favorable environment for misconduct and abusive behavior by mala fide agents and for infiltration of money launderers into the payment services systems.

In most cases, money laundering in the payment services sector involves conspiracy of agents with money launderers. It is most likely that money launderers commit a wide range of predicate offences such as tax evasion; illegal receipt of the budget funding; active and passive bribery; fraud, including financial fraud; payment of salaries off the books, etc. Money laundering is facilitated by the fact that it is extremely difficult to ensure continuous monitoring of the agents. It is impossible to definitely establish whether or not an agent has received cash from an individual payer or a wire transfer from a criminal scheme organizer, since the different stages of such schemes are often implemented through different credit institutions.

The significant improvement achieved in recent years, was imposition of the obligation on the agents to deposit all received cash into the special bank accounts. However, the operators face objective difficulties in course of monitoring of the use of such special bank accounts by their agents. In a situation where the agency networks are widely extended across the regions, the use by an agent of the special bank account opened with the principle bank is becoming the exception rather than the rule. Replenishing the balance on agent current account may be impeded by complexity of sub-agent settlements, by the need to take loans against floating (working) capital and by other objective factors.

In this context, on-going monitoring of agency payments as they pertain to the providers of goods and services for the benefit of which the agents accept funds from individuals becomes critical for ensuring efficient oversight for the AML/CFT purposes. The powerful deterrent to misuse of agency arrangements for money laundering purposes is the threshold amount of 15 thousand rubles established by the law in relation to transactions that can be carried out without identification. To launder large amounts of funds through an agency network, perpetrators take advantage of regular smurfing, which is one of the distinctive indicators of money laundering. Thus, detection of splitting of a large amount of money is the clear indicator of a potential breach of the law (of commission of a crime).

Despite a wide variety of typologies of money laundering through the agency networks, one can identify a number of control points for timely detection and deterrence of transactions that pose enhanced risk of money laundering. First of all, it involves controls implemented by the operators. Developed for monitoring of this part of the payment chain should be the technique for assessing reliability and loyalty of agents. This should include verification of date of government registration and date of commencement of business operations of an agent; verification of its authorized capital; verification of whether or not the registered address of an agent is shared by large number of other entities and/or whether or not an agent is founded and managed by persons who are the founders and managers of a large number of other entities; fit and proper test of the senior management and their knowledge of the payment services regulations; verification of whether or not the amounts of performed transactions are consistent with the available infrastructure (number and location of terminals, availability of business premises, qualified personnel, etc.); verification of information on business operations, financial standing and business reputation of an agent against publicly available data, etc.

Besides that, it is necessary to grade the recipients of transfers and payments in terms of risks posed by them. The high-risk recipients should be identified and closely monitored. In particular, it is necessary to regularly (at least once a month) and thoroughly analyze the amounts and nature of transactions carried out for the benefit of the high-risk recipients. Such recipients may include recipients unknown in a given goods or services market and also entities that accept funds and further credit/ deposit them into customers' accounts and allow such customers to freely use the deposited/ credited funds as they wish without restrictions.

The results of such monitoring and analysis should allow for detecting the cases where transactions carried out for the benefit of the high-risk counterparties (e.g. credit institutions) are split. The "smurfing factor" can serve as a convenient indicator which is calculated as a ratio of total amount of funds accepted during a given period for the benefit of recipients of a counterparty to a number of bank accounts of the recipients multiplied by 15 000. The experience shows that if the smurfing factor value is close to 1, it indicates that split transfers/transactions start to prevail. Transfers of funds for the benefit of the same or similar recipients, having the common

nature, are featured by the average value of the aforementioned smurfing factor. Comparison with this average value allows for detecting significant deviations of this indicator which points to unreliable agents.

The efficient way of preventing smurfing of large-value transactions is the establishment of thresholds of total value of transfers per one recipient account during a given period of time (in practice, during a month) through an agency network. Such threshold may differ depending on a risk posed by a recipient and its service, but the recommended average threshold is around 100 thousand rubles per one recipient account per month. And deviation from the defined parameters should be detected by the monitoring and oversight system for further verification and assessment of the nature of the detected payment(s). In-depth analysis of the incidents will allow for establishing, within the shortest time, the properly operating system for detecting illegal transactions with further reporting them to the competent authorities and also for defining the relevant monitoring parameters to be regulated.

The presented approaches to analysis of operations of agents involved in provision of payment services will facilitate the establishment of the efficient system for monitoring agent operations for the AML/CFT purposes.

NEW RUSSIAN LEGISLATION PROHIBITING CERTAIN OFFICIALS FROM HAVING FOREIGN BANK ACCOUNTS IN CONTEXT OF INTERNATIONAL BANKING BUSINESS

Tamara S. Kozodoy,
international analyst, PhD

New legislative initiatives implemented in Russia last year could not but produced certain impact on policies of foreign banks operating in this region and dealing with the Russian customers. The main changes in the Russian legislation that drew attention of the international banking community were outlined by President Putin in his annual address to the RF Federal Assembly on December 12, 2012. "How can the public have confidence in an official or politician who talk about the national development and prosperity, but at the same time tries to withdraw his money and assets out of the country? I request you to support the legislative proposals limiting the rights of the national officials and politicians to hold foreign bank accounts, securities and stock". This statement was greeted with applause, but the Presided added: "Hold your applause, you may not like what is coming".

Following publication of this address, the international financial institutions, that strived to comply with the requirements of the national regulators in a situation where they faced severe competition in the international financial markets, could anticipate the implications of the expected changes in the Russian legislation and started to revise their business practices in respect of the Russian customers. Such revision took place in parallel with the development of draft Federal Law No.79-FZ *on Prohibition to Certain Categories of Citizens to Open and Hold Accounts (Deposits), Keep Cash Funds and Valuables in Foreign Banks Located outside the Russian Federation, to Own and (or) Use Foreign Financial Instruments* (hereinafter Federal Law No.79). By the time of enacting of Federal Law No.79 on May 7, 2013, foreign banks could develop their own vision of the changing legal

environment and assess the main risks related to such changes. It is noteworthy that foreign banks quite often took a preventive approach to the new Russian Law, i.e. their position was based not on the final text of the Law and its practical enforcement in Russia, but on the political rhetoric and debates in course of its development which they could closely monitor.

This article analyses a range of issues that, in the opinion of its authors, are important for correct interpretation of the basic provisions of the Law.

In the interpretative note to the draft law the Present clarified that "the prohibition is imposed for ensuring the national security of the Russian Federation, regulating the lobbying activities, attracting investments in the national economy and enhancing efficiency of the anti-corruption efforts". By comparing these objectives with the text of Federal Law No.79 and with a number of formal comments made in the State Duma, one can make conclusions about the main goals pursued by the new law:

- **Combating corruption and related money laundering:**
  Despite the relatively soft sanctions enforceable under the Law, it still provides for implementation of preventive and oversight measures through the government supervisory regime under which the officials and their affiliates may use and dispose of their assets.

- **Fighting against tax offences and related outflow of capital:**
  The aim of Federal Law No.79 is to limit possible withdrawal by certain officials of their assets and savings from the Russian banking system which will prevent tax evasion and outflow of capital abroad through various offshore arrangements. The new Law also promotes the law-abiding behavior among the Russian elite - the officials are required to comply with high business conduct standards, which, in its turn, will encourage the business community to invest funds, develop adequate corporate management systems and pay taxes in the Russian Federation.

Foreign financial institutions pay special interest in potential exterritorial application of Federal Law No.79. In principle, foreign financial institutions are not obliged to comply with the Russian laws, since these laws are binding only upon those individuals and entities that are subject to the RF jurisdiction. Therefore, Federal Law No.79 formally applies only to the officials and their close relatives, and their compliance with this Law is ensured through a range of oversight and detective measures

implemented by the relevant national government authorities.

At present, the principle of territorial application of law is challenged following the adoption of 2010 UK Bribery Act and US Foreign Account Tax Compliance Act which establish the principle of long arm and set requirements for foreign financial and non-financial institutions. No such principle is established by Federal Law No.79. So far, Russia has not fully implemented one of the most effective mechanisms for enforcement of the "extraterritoriality principle" – putting pressure on foreign institutions by threatening to close or limit their access to the domestic financial markets.

Nevertheless, the aim of the Russian legislators is to ensure actual compliance by foreign financial institutions with the new prohibition. Article 10 of Federal Law No.102-FZ on amendments to certain RF legislative acts following adoption of Federal Law No.79 (hereinafter Federal Law No.102) authorizes the federal AML/CFT agency (Rosfinmonitoring) to inform, in coordination with the RF Central Bank and in a manner prescribed by the RF President, the foreign competent authorities on the established prohibition for implementation by the latter of the FATF Recommendations. There are also the international instruments (including those adopted by the UN, Council of Europe and OECD) that prohibit financial institutions from facilitating withdrawal of assets abroad and use of such assets in breach of the ant-corruption and tax legislation. Such measures are also implemented within the national legal frameworks. Therefore, Russia may expect that the objectives of the recently adopted laws will be successfully achieved provided that these laws are correctly understood by foreign financial institutions.

Federal Law No.79 does not impose any criminal or administrative sanctions against persons who breach its provisions. Failure to comply with the Law may result in early termination of powers, resignation or dismissal from office due to loss of confidence. Thus, unlike commission of predicate offences underlying money laundering, non-compliance with the said Law does not entail imposition of sanctions and enforcement actions under the international and national legislation.

In this context, foreign financial institutions assess the consequences of possible breach of Federal Law No.79 by their Russian customers primarily in terms of the reputational risk and non-compliance with the regulatory requirements. Foreign banks may be more sensitive to the reputational risk than can be affected by failure to comply with the said Law (as opposed to tax crimes), since Federal Law No.79 is directly related to their core business – maintaining customers' accounts.

In general, the attitude of banks towards their customers affected by Federal Law No.79 may be divided into three categories, depending on level of the reputational risk:

- *Restrictive approach* involving termination of business relationships with the Russian customers who are politically exposes persons (PEPs);
- *Formally conservative approach* that may involve termination of business relationships with the customers formally covered by Federal Law No.79;
- *Liberal approach* that does not involve proactive closing of accounts and termination of financial transactions with such customers and lays the burden of compliance with the national laws on the Russian customers.

Determination of the acceptable level of the reputational risk and, hence, selection of a particular approach by a financial institution depends on the policy of the national regulator, stability of business, importance of the "Russian sector" in operations of a bank, availability of key customers covered by Federal Law No,79 and other factors.

Practical enforcement of the new Law in Russia has not been established yet, and the "rule of the game" is not fully understood by the external (foreign) players. So far, information published in mass media, including comments of the Russian experts and officials, has not always helped banks to clearly understand new instructions and regulations. In a situation where there are no sufficient and clear guidelines for practical implementation of the new Law, financial institutions operating in jurisdictions with high regulatory and self-regulatory standards may prefer to apply the restrictive or formally conservative approach in respect of the Russian customers and their financial transactions.

One can identify a number of issues that may pose a challenge for foreign banks in practical implementation of the new regulations.

- The concepts used in Federal Law No.79 for defining persons who are subject to

the prohibition require professional legal interpretation.[1] Financial institutions should clearly and correctly distinguish between the closely related legal terms used in the Russian legislation, such as "state position (job) in the constituent regions of the Russian Federation", "position in the federal government agencies", "position in the government-owned corporations established under the federal laws", etc. Since many foreign banks lack sufficient resources for adequate interpretation of the provisions of the Russian laws, they have to consult with the publicly available information sources which often appear to be misleading and controversial.

For example, one month prior to enactment of Federal Law No.79, many Russian Internet sites quoted the official statements that the ban to hold foreign bank accounts also applied to the directors of such government monopolies as Gazprom and Rosneft. However, the adopted Law does not apply to many government monopolies since such monopolies have not been established under the federal laws and, therefore, cannot be considered the government corporations as defined by Article 7.1 of Federal Law No.7-FZ on Non-Profit Organizations dated January 12, 1996.

In compliance with the goals of the Law, outlined in the aforementioned presidential address and defined in Article 1 of Federal Law No.79 as "establishing ban for persons who take, in course of discharging their duties, decisions related to the sovereignty and national security of the Russian Federation", it appears logical that members of the Russian legislative authorities are also prohibited from opening and holding foreign bank accounts. Pursuant to Federal Law No.102 similar prohibition is applied to persons holding state positions (jobs) in the RF constituent regions and to their spouses and minor children. Article 12 (par. 3-9) of Federal Law No.184-FZ of 06.10.1999 *on General Principles of Organization of Legislative and Executive Authorities of the RF Constituent Regions*, as amended following adoption of new laws pertaining to foreign accounts, stipulates that restrictions apply to the members of the legislative assemblies elected in the single-member and multi-member constituencies as well as elected by the party-list system, which is reasonable, since members of the local legislative assemblies are included in the aforementioned list of state positions (jobs) of the RF constituent regions. However, not all members of the legislative authorities of the RF constituent regions fall in the category of persons holding state position (job) – these issues are regulated by the legislation of the constituent regions.

For example, all members of the legislative assembly of Primorye Territory are included in the list of persons holding state position (job) of this region (Art.2 of Primorye Territory Law No.87-KZ of 13.06.2007 on State Positions (Jobs) in Primorye Territory), while in Perm Territory, only those members of the legislative assembly who work on a permanent (professional) basis are considered the persons holding state position (job) (Art.5 (par.1) of Perm Territory Law No.9-PK of 06.03.2007 on Status of Member of Perm Territory Legislative Assembly).

- Federal Law No.79 defines categories of persons who are prohibited from "opening and holding accounts (deposits), keeping cash

[1] List of persons affected by Federal Law No.79:

a) Persons holding a state position (job). A full list of sate positions (jobs) is provided in the RF President Decree of January 11, 1995, as further amended;

b) First deputy and deputies of the Prosecutor-General of the Russian Federation;

c) Members of the Board of Directors of the Central Bank of the Russian Federation;

d) Persons holding a state position (job) in the constituent regions of the Russian Federation. A full list of sate positions (jobs) in the Constituent regions of the Russian Federation is provided in the RF President Decree of December 4, 2009;

e) Persons appointed by the RF President, the RF Government or the RF Prosecutor-General to positions in the federal government agencies (as per the Federal Law on Public Service);

f) Deputy directors of the federal government agencies;

g) Persons appointed by the RF President or by the RF Government to positions in the government-owned corporations, foundations and other organizations established under the federal laws;

h) Heads of municipalities and urban areas;

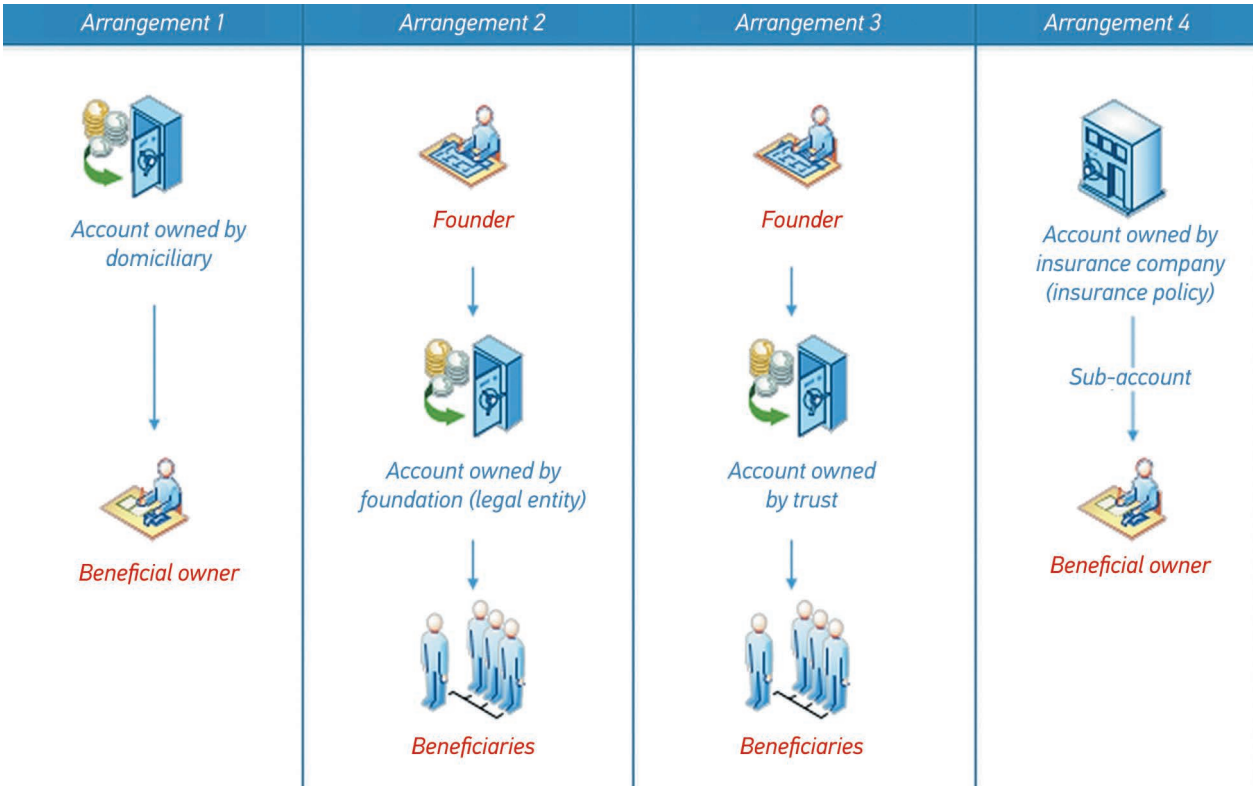
i) Spouses of the above persons and their minor children.

funds and valuables in foreign banks located outside the Russian Federation, and owning and (or) using foreign financial instruments" (Art.1).

It is very important for financial institutions to correctly interpret the terms "open accounts (make deposits) and "hold accounts (deposits)". Where these terms apply only to an account holder, then, for example, an account opened by a foreign bank for a domiciliary which beneficial owner is the Russian official will not constitute the breach of Federal Law No.79. If the prohibition also covers beneficial owners, the question then arises as to whether or not the restrictions apply to authorized persons who have access to such account.

Similar challenges occur when an account is opened through trusts (or similar corporate arrangements). Funds invested in a trust are legally separated from the founder, but at the same time are not owned by the trust beneficiaries. Thus, it is impossible to determine who actually "opens and holds" such accounts without further clarification. Presented below are several examples of bank account arrangements that require clarification of the terminology used in Federal Law No.79.

Since it is very difficult to ensure efficient implementation of the recently adopted Russian laws without international cooperation, Russia (as the country) as well as foreign banks and their Russian customers may be interested in further clarification of the laws and their enforcement practice which can be done by modifying the relevant legislative provisions and issuing legal comments related to the newly adopted laws.



INFORMATION ABOUT FEDERAL LEVEL EVENTS

V. PUTIN: "DAMAGE ONLY FROM THE DETECTED CRIMES COMMITTED IN THE DOMESTIC CREDIT AND FINANCIAL SECTOR OVER THE LAST THREE YEARS AMOUNTED TO MORE THAN 20 BILLION RUBLES"

President of the Russian Federation hosted a meeting at the Rosfinmonitoring dedicated to combating illegal financial transactions in the banking sector and visited the National Security Risk Assessment Center for Anti-Money Laundering

Irina V. Ivanova,
Editor in Chief

On 4 March 2014, the President of Russia V.V. Putin paid a visit to the Federal Financial Monitoring Service, where he chaired a meeting dedicated to combating illegal financial transactions in the banking sector. Prior to the start of the meeting, the President took time to inspect the Risk Assessment Center, which had opened its doors at the agency only a few months before following the June 2012 presidential decree that transferred the functions of the national center for assessment and combating the threats to national security arising from money laundering, terrorist financing and proliferation of weapons of mass destruction to the Rosfinmonitoring. Yu.A. Chikhanchin, director of the Russian Financial Intelligence Service, informed participants about the activities of the Center and its first results.

«The Centre has been operating for only three months now, and it is very much at the start of its journey,» said Mr. Chikhanchin, noting that the center is «a special mechanism that allows the authorities to see at an early stage the processes that occur inside the financial industry and take a preventive action before criminal prosecution becomes inevitable».

What makes this Center unique is that in its work it utilizes the information about payments made by customers of financial institutions, i.e. highly reliable information.

The Center analysts have identified six major areas of risk. The first deals with the international component.

«Basically, those are the things connected with possible sanctions against Russia, say, through the UN Security Council, OECD or FATF, and they are the transactions we monitor particularly closely,» explained the Rosfinmonitoring director.

«The second area relates to risks associated with the activities of financial institutions. Our work here is carried out in close contact with the Central Bank, which allows us to anticipate possible negative processes occurring inside financial institutions. The third area covers risks associated with industries. Additionally, we also track risks associated with the regions,» said Yury Chikhanchin.

A separate group of risk is associated with social tensions linked to terrorism and extremism.

In his opening remarks at the meeting, V. Putin stressed the importance of making maximum use of the information and operational capacity of the Centre, and on this basis to more effectively counter illegal financial transactions.

V. Putin:

Recently, we have taken several important steps to improve the national legislation in this field. One of them was the enactment of the law on combating illegal financial transactions. It expanded the powers of credit institutions and supervisory bodies and, at the same time, increased their responsibility for decisions and results. The work to suppress organizations involved in money laundering and improve transparency of financial institutions is proceeding at a healthy pace.

These efforts have received their deserved recognition also at the international level, including from the FATF, which described our anti-money laundering and terrorist financing system as one of the best. This year is the year of the Russian presidency at the FATF, and we intend to use it to intensify contacts with our colleagues there.

We still have much to do both at the international and national level. Here let me give you just a few numbers. According to law enforcement, more than 42,000 crimes were committed in 2013 in the domestic credit and financial sector, of which nearly 16 percent involved large and particularly large amounts. The extent of the damage only from the detected crimes committed in the domestic credit and financial sector over the last three years amounted to more than 20 billion rubles.

These are the areas that we, I believe, should focus on. First, it is necessary to consolidate the efforts of the agencies responsible for combating illegal financial operations and improve the overall quality of work in this area. Separately, I would like to emphasize that with the opening of the center we now have the opportunity to spot problem areas and forecast future developments. Therefore, the emphasis should be placed on early-warning measures and preventive actions. Of course, we should actively involve in this work the federal subjects and their leaders.

In this regard, it is important to develop the concept and clear rules of interaction for all agencies utilizing the potential of the center, i.e. the Rosfinmonitoring, Bank of Russia, law enforcement and other agencies. And, of course, the resources and opportunities created by the center constitute an important tool for dealing with the task of deoffshorization of our economy, which was set in my Address to the Federal Assembly, in particular for obtaining information about the ultimate beneficiaries of offshore companies.

I and Elvira Sakhipzadovna [Nabiullina] have just taken a look at the opportunities offered by the center in this area, which I find pretty impressive. We just need to use them properly.

Second. It is necessary to accelerate and qualitatively change the work aimed at improving the legal framework for combating illegal financial transactions. I repeat: the adoption of the Federal Law 134 is a big step forward, but we must remember that the activities of various illicit financial entities are becoming increasingly sophisticated today and criminals exploit the smallest legal inconsistencies in order to execute their criminal schemes and evade responsibility for them. We must quickly close gaps in legislation, act proactively and consistently. Now I would like once again to go back to those information capabilities that we have witnessed today: the equipment we have there offers great possibilities for all people present here, bearing in mind that the system works in real time.

We have recently discussed some of the aspects of this work at a meeting with members of the government. In particular, we recalled that the government still hasn't enacted the regulations that would increase criminal liability of financial institutions for providing false financial statements. This has to be done. At the same time, I want to emphasize that honest enterprises should not suffer from excessive, redundant and, sometimes, on-paper-only checks, which is something we talked about many times before. These checks, and we all know it, make very little practicable difference, only working to create additional problems for law-abiding businesses, companies and banks.

ROSFINMONITORING REPORTS 2013 RESULTS

On 7 March 2014, Rosfinmonitoring hosted a closed meeting of the Collegium of the Federal Financial Monitoring Service titled "On Performance of the Federal Financial Monitoring Service in 2013 and Primary Objectives for 2014".

Irina V. Ivanova,
Editor in Chief

In his opening remarks, Rosfinmonitoring Director Yu. A. Chikhanchin outlined a new direction for the assessment of performance of the financial intelligence unit: from official statistics towards a comprehensive analysis of the economy through the introduction of early warning mechanisms to guard against violations of anti-money laundering law.

When delivering a keynote address, Rosfinmonitoring Deputy Director V. I. Glotov reminded the participants of the complementary remarks made by the Russian President Vladimir Putin during his visit to Rosfinmonitoring in March 4, 2014 about its work aimed at identifying risks and threats to the national security and about the impressive operational and information capacity of the Risk Assessment Center. Among the main outcomes of the work of the national anti-money laundering and terrorist financing system in 2013 were a successful defense of the Follow-up Report of the Russian Federation before the FATF experts and the adoption of the Federal Law No. 134–FZ, made possible due in no small part to the concerted efforts of all stakeholders, including in the framework of the Interdepartmental Working Group on Combating Illegal Financial Transactions (IWG), created by the President of the Russian Federation on July 31, 2012 and for which information and analytical support is provided by Rosfinmonitoring.

The IWG undertook targeted coordinated measures to tackle the largest illicit platforms for illegal financial transactions, particularly in the Republic of Dagestan and the Samara region, undermining the infrastructure for illegal financial transactions in the Samara region and achieving an almost 90-fold decrease in the number of monthly suspicious transactions.

The IWG also studied the issue of existence of stable illicit banking channels for moving funds under fictitious foreign trade contracts concluded

with Belarusian and Kazakh companies. In this regard, the IWG decided to undertake a comprehensive analysis of the implementation of decisions of the Eurasian Economic Commission and use its results in the preparation of proposals for improving the customs and exchange control mechanisms governing trade between residents of countries member-states of the Customs Union for consideration by the Supreme Eurasian Economic Council.

The number of organizations registered with the financial intelligence unit grew by approximately 2% in 2013 vs. 2012 to exceed 24,000. The volume of data coming from real estate agents went up by almost 50%, driven by both rising entity numbers, including new individual entrepreneurs, and improved quality of Rosfinmonitoring's internal controls and supervision measures.

The main suppliers of reports on transactions with monetary funds and other assets in 2013 were credit institutions, accounting for about 95% of all incoming messages. As of December 1, 2013, there were 930 credit institutions and 2037 branches operating in Russia.

The task facing the entire Russian anti-money laundering system today is to improve performance of all of its members: the FIU, the Bank of Russia, law enforcement, tax and oversight agencies, and the private sector. All this should help cure the ailments and improve the health of the Russian economy.

2013 saw a drop in the number unscrupulous lending institutions. Thus, the number of banks and their branches decreased by 10.2% vs. 2012 (26 banks and 312 branches), with the North Caucasus Federal District accounting for the biggest share of casualties in the banking sector – 14%. The number of branches in the Volga Federal District went down by 23.6%, due, among others, to the busting of the illicit currency conversion platform in the Republic of Dagestan and the Samara region.

Despite the falling numbers of credit institutions and their branches, the number of transaction reports coming from them in 2013 actually increased by 3.2 % vs. 2012.

Compared with the last year, the direction of Rosfinmonitoring's activities in the priority areas of financial intelligence has remained largely unchanged: Rosfinmonitoring continued to strengthen its efforts aimed at countering the threats to the country's budget.

While working in close cooperation with Rosfinmonitoring, law enforcement authorities successfully foiled a number of large-scale illegal financial schemes.

The total number of ML financial investigations in 2013 continued to grow: by 11% vs. 2012.

While working in close contact with the Bank of Russia, the Main Directorate for Economic Safety and Counteracting Corruption of the Russian Interior Ministry and other law enforcement authorities, Rosfinmonitoring put an end to the work of an illicit cash conversion platform that had operated for several years at one of the banks. In total, over a period from 2010 to 2013, that system was used to convert into cash several hundred billion rubles.

This bank was in fact a veritable «conversion factory», whose services were popular with both criminals and other intermediary banks. The scale of this criminal activity was so impressive, and the scheme was so expertly run that the fallout from its demise had a profound impact on the country's entire banking system and is still being felt.

The number of cases featuring materials provided by Rosfinmonitoring that were referred to courts remained largely the same as last year, except for a 41% increase in cases initiated under Articles 174 and 174.1 of the Criminal Code.

As of January 17, 2014, a total of 3297 legal entities and individuals had been added to the List of entities and individuals known to be involved in extremist and terrorist activities, of which 2796 individuals from the Russian list were either investigated on extremism and terrorism charges or found guilty of these crimes; and 52 terrorist and extremist organizations whose activities in Russia have been outlawed by the Supreme Court of the Russian Federation and in respect of which the court has issued liquidation or prohibition orders. The international list contains 367 individuals and 82 organizations (as per UN Security Council resolutions).

In his speech, P. V. Livadny, State Secretary and Rosfinmonitoring Deputy Director, recalled that in September 2014 Russia would report to MONEYVAL, which would require maximum effort not only from the FIU, but also every and each member of the national anti-money laundering system.

When summing up, Rosfinmonitoring Director Yu. A. Chikhanchin spoke about the importance of understanding the meaning of efficiency, on which the success in achieving by the country and its legal and institutional systems of the expected results depended. It is through the prism of these goals that the 2014 targets were set for the entire Agency.

V.I. Glotov, Rosfinmonitoring Deputy Director

BUSINESSMEN AND GOVERNMENT CUSTOMERS ARE UNDER ROSFINMONITORING'S MICROSCOPE

On 5 March 2014, during the Government Hour of the Federation Council of the Federal Assembly of the Russian Federation, Rosfinmonitoring director Yury A.Chikhanchin addressed the senators

Konstantin V. Litvinov,
Deputy Chief Editor

Recalling the key milestones for 2014 set in his December 2013 address by the Russian President Vladimir Putin, Y. A. Chikhanchin stressed that one of the main tasks facing the country's economy is to improve its transparency: understanding the real state of the banks and financial institutions in general, as well as cleansing them of the «dirty money», i.e. elimination of the so-called «laundry shops».

Y.A. Chikhanchin said that the adoption last year of the Federal Law No 134-FZ has allowed Rosfinmonitoring to significantly amend several provisions of the anti-money laundering legislation concerning multiple areas. The next step must be to confirm the effectiveness of the existing mechanism, and Rosfinmonitoring director expressed confidence that it will be done.

Speaking of the 2013 performance highlights, Y.A. Chikhanchin noted that the agency was able to significantly reduce the level of banks' involvement in large illicit schemes, achieved among others through license revocations; to focus the activities of authorities involved in the anti-money laundering system on finding solutions to the main problem: combating the activities of «laundry shops»; and to identify the industries and regions most susceptible to illicit schemes, which became possible thanks to establishment of Rosfinmonitoring's Risk Assessment Center.

As of now, according to Rosfinmonitoring director, the agency has identified six major risks: international, financial institutions, industries, regions, budget and risks connected with the financing of terrorism and extremism. For each of these areas, Rosfinmonitoring has developed criteria that, when combined, allows for the identification and, whenever possible, prevention of risks.

After his opening speech, Y.A. Chikhanchin fielded questions from the senators. Some of them are given below.

M. H. Suyunchev, a member of the Federation Council Committee on Budget and Financial

Markets, a representative of the legislative (representative) body of state power of the Republic of Karachay-Cherkessia in the Federation Council

– Yury Anatolyevich, I have a question concerning the Council of Heads of CIS Financial Intelligence Units. What is currently being discussed there?

Y.A. Chikhanchin: To begin with, its members are discussing ways to integrate our information resources. We are very close economically and integrated financially through the banking sector, meaning that by pooling our resources together and undertaking joint financial investigations we should, in my opinion, solve a few problems. Only a few days ago we together with Kyrgyzstan opened a criminal case against a group of couriers who were involved in the smuggling of tens of millions of rubles whose origin is yet to be traced. As of now, we and our colleagues from Tajikistan, Uzbekistan and Belarus have identified several financial centers serving drug traffickers.

Stepan Kirichuk, chairman of the Federation Council Committee on the Federal Structure, Regional Policy, Local Government and Northern Affairs, a representative of the executive body of state power of the Tyumen region in the Federation Council

– Yury Anatolyevich, please tell us what measures are being taken by Rosfinmonitoring to combat illegal cash-out transactions?

Y.A. Chikhanchin: I consider them a great evil for any country, because large volumes of cash circulating in the economy tend to create conditions conducive to its criminal misuse. 7% of the turnover is rather a lot, and clearly this is the money that can be put to a better use. To address the problem, today we are launching an early warning mechanism. I believe we should have measures in place that would allow us to «kill off» an illicit cash-out center while it is still in its infancy, rather than wait for five or six years.

Every bank that comes on the radar for its links to suspicious firms or suspicious transactions receives a message from us, saying: «You have a problem, dear bank manager». About 90 percent of banks will react quickly and take steps to put things in order. In

some cases, we also notify regional governors and presidential envoys, especially if the banks in question hold government money and regional budgetary funds. They also hold meetings and discuss ways how to deal with specific cases. I believe, this basic prevention mechanism works better than criminal prosecution

Y V. Shamkov, first deputy chairman of the Federation Council Committee on Economic Policy, a representative of the executive body of state power of the Altai Territory in the Federation Council

– Dear Yury Anatolyevich, in your speech and previous answers you have already touched on this topic a bit, but nonetheless. Could you let us know what major challenges you are currently working on together with the Bank of Russia?

Y.A. Chikhanchin: The main challenge we are working on today concerns, of course, the regulation of activities of financial institutions and customers. Since becoming a mega-regulator, the Central Bank has become responsible for the regulation of numerous financial institutions that in the past reported to other supervisors, including Rosfinmonitoring. This is perhaps our biggest challenge: to build an efficient regulatory mechanism. The second challenge is to develop a common approach to supervision. This is necessary because, unfortunately, as it turns out, even we, the supervisors, do not always correctly interpret regulations, meaning that for the same offence different supervisors may mete out different punishment. This is not right. And this leads to disagreements between supervisors, which are exploited by some in the business community, and to unfair rules for businesses. I believe sorting our regulation is paramount.

Next challenge is to ensure early detection of these negative trends in financial institutions and their supersession, albeit not through liquidation, but rather through warnings and alignment of mechanisms.

And the last challenge is to increase financial literacy among employees of financial institutions. In my opinion, they should primarily play a role of financial advisors, and not financial usurers. And they also need to help people. Second, it is important to educate the public. We, unfortunately, suffer from the fact that many people do not know how to build relationships with financial institutions. It is for this illiteracy that we often have to pay a heavy price, like the price we paid for Master-Bank and others: 10 billion in maternity capital, of which 80% went to criminals and only 20 to the people who needed it. We must educate the public. It is our job as a mega-regulator.

Oleg A. Kazakovtsev, a member of the Federation Council Committee on Budget and Financial Markets, a representative of the legislative (representative) body of state power of the Kirov region in the Federation Council

– Dear Yury Anatolyevich, what current risks does Rosfinmonitoring see in the banking sector? Is it possible to somehow warn, take proactive action or notify customers of risks, because it is only depositors who are compensated later, not the rest of the customers? And question two: given that today even our state-owned companies are involved in offshore schemes, what is in you estimate the percentage of these companies?

Y.A. Chikhanchin: I must say that in last two years we have been very proactive in our work with companies with state participation. As you may remember, following the events at the Sayano-Shushenskaya HPP, the president issued a decree requiring all state-owned companies to report to Rosfinmonitoring, thereby changing the situation considerably. Our investigation revealed that money was siphoned abroad and the management used affiliated structures.

The most important thing is that many companies and corporations with state participation have by now established internal oversight mechanisms similar to Rosfinmonitoring's, among the most noteworthy of them are Rosatom, which developed a mechanism that allows it to track all transactions and suspend them if necessary, Rosneft, Rostechnologies, Aeroflot, etc.

As far as early warning mechanisms are concerned, again here, I think, we must first raise the degree of financial institutions' liability for being dishonest with their customers and for taking part in shady schemes. Revocation of licenses is, of course, a very bad thing. After all, when the owner loses his license, I don't think he will rue its loss all that much, given that most of his money would be abroad, in good banks with impressive reputation. The focus here should be on increasing liability of individuals, be it owners, managers or those who participated in the fraud.

***

After answering the questions from the senators, Rosfinmonitoring director was presented with the Federation Council. 20 Years medal by **Federation Council Chairwoman V I. Matvienko.**

«We highly appreciate the work you do. I have visited Rosfinmonitoring and saw with my own eyes how modern the center that you have set up is and how modern the approaches the agency uses in its work, not only in terms of oversight, but also in terms of new initiative and ideas, including on how to improve legislation. It also became clear to me that Rosfinmonitoring keeps a close eye on all financial market participants, a very close eye indeed.»

I would like to take this opportunity to appeal to the representatives of the business community and government customers: do not break the law! They turn the screen on and see every firm: where it paid, how it paid and where the money went. Therefore, it is much better to be on good terms with the law and play by the rules. We are all under Rosfinmonitoring's microscope, let's not forget about it.

GOVERNMENT PROCUREMENT: THE SPHERE MOST SUSCEPTIBLE TO CORRUPTION

In December, 2013 anti-corruption conference arranged by the Moscow Government and supported by the International Business Leaders Forum (IBLF) was held in Moscow. The event concurred with the 10-th anniversary of the United Nations Convention against Corruption (UNCAC)

Irina V. Ivanova,
Editor in Chief

Shannon Bullock, a representative of the United Nations Office on Drugs and Crime, in her welcoming speech emphasized the importance of efforts taken by different states in countering the problem. N.A. Sergunina, Moscow's Deputy Mayor for Economic Policy, Property and Land Relations, recalled that corruption is a global problem, not just Russian. And each country tries to solve it in its own way.

The participants made different suggestions aimed at making the procurement procedures as transparent, open, impartial and affordable as possible, including public control as well as transferring all government procurement-related procedures into electronic form. Especially as similar intermediary-free system is already in operation in the building sphere.

The issue of direct combating corruption was touched upon in the speech of Rosfinmonitoring First Deputy Director Yu.F. Korotky. He recalled that Financial Intelligence has been effectively cooperating with the Moscow Government for a long time, and it passes tendering procedures at the stage of applicants selection as well as during contracts execution and when spending allocated funds.

Yu.F. Korotky recalled the meeting of law enforcement authorities held at the Prosecutor General's Office in November, 2013 summarizing the results of execution of the National Anti-Corruption Plan approved by the RF President Decree No. 297 of March 13, 2012. At this meeting the sphere of government procurement had been referred to as «the sphere most susceptible to corruption».

«This appears to be the case,» he continued, «since the sphere of government procurement involves a whole bunch of corruption risks joint in a special way - actually, all attributes of corruptogenic situation

are available: potential perpetrator of corruption - public officer, the target of corruption, being the most susceptible to corruption - budgetary funds, and, finally, the point is that the perpetrator and the target are involved in a vulnerable system of relations, where the public officer allocates budgetary funds and is in charge of the procurement procedure, including selection of the supplier or general contractor.»

According to the first deputy Financial Intelligence Director, as to combating corruption in the procurement sphere, one should talk about the ways of localization of risk factors or at least minimizing their impact - that is, prevention and preclusion of corruptive behaviour of the officer; ensuring control over effective spending budgetary funds, excluding their utilization for the purpose of corruption; and, finally, ensuring transparency and openness of the procurement procedures themselves at all stages of the government contract lifecycle. As for the latter, this is the target of provisions of the Federal Law No.44-FZ coming into force and effect since January 1.

Everyone is well aware that Rosfinmonitoring, besides procurement procedures management, conducts so-called «contingent-oriented» work - monitoring of financial transactions involving persons who hold state posts as to the completeness and credibility of information declared by these persons concerning their income, expenditures, movable and immovable property, foreign bank accounts, participation in business management, etc. It should be mentioned that there is a separate international AML/CFT standard concerning control over transactions involving politically exposed persons among the 40 FATF Recommendations (Recommendation 12).

«The main thing here is not to make the control total,» emphasized Korotky, «clear corruption risk indicators are required to which the system should be tuned and to which it should respond.»

Yu.F. Korotky: «Financial monitoring system is tuned to the indicators of income derived from corruption. Generally, we suppose that the notion of «income derived from corruption» is the key concept not only for understanding corruption as phenomenon but also for practical revealing of corruption mechanisms, since corruption is based on seeking lucre, and corruption practice is actually deriving personal gain. For our authority - the Federal Financial Monitoring service - the notion of income derived from corruption is twice more important, since, in addition, it is income derived from corruption that is being legalized (laundered).»

Today budgetary funds are items of the highest risk. Yu.F. Korotky recalled the story of purchase of

Yu.F. Korotky, Rosfinmonitoring First Deputy Director

64-slice computer tomographs. That was one of the first experiences of targeted financial monitoring according to object-based corruption indicator.

Yu.F. Korotky: At that time prices for the same type appliances produced by General Electric or Toshiba, with manufacturer's price starting from 16 mln. Rub. amounted up to 95 mln.Rub. Profit of the intermediary (that is, income derived from corruption) was 50-60 mln rubles on the average per one item. In total over 3 bln rubles were then dissipated all over the country. Over 130 criminal cases were initiated in 54 regions of the country, 96 managers were prosecuted, including 30 former and acting regional.

Health Ministers of the subjects.Summarizing, Rosfinmonitoring First Deputy Director said: «Law enforcement officers will agree with me that the most complicated thing in combating corruption is exposing the corruptionist which had not been caught red-handed in due time. Especially when income derived from corruption is transferred abroad. Until recently such cases were non-detectable. Now, when operations and transactions involving foreign politically exposed persons are to be disclosed by banks, realtors and other financial intermediaries, subject to FATF Recommendation, the situation is changing, and foreign assets are being traced more frequently.»

INTERNATIONAL NEWS BLOCK

FATF PLENARY MEETING IN PARIS

Under the Russian Presidency (V. P. Nechaev), the meetings of expert and working groups as well as the Plenary meeting of the Financial Action Task Force (FATF) were held in Paris on February 9-14. The meetings were attended by the Russian interagency delegation headed by Rosfinmonitoring Deputy Director V. I. Glotov and representatives of the Secretariat of the Eurasian Group on Combating Money Laundering and Financing of Terrorism (EAG)

Irina V. Ivanova,
Editor in Chief

The main issues on the agenda were:

- approving universal procedures for conducting anti-money laundering and counter-terrorist financing mutual evaluations by all assessment bodies based on the FATF 2013 methodology;
- preparing for the fourth round of mutual evaluations;
- updating the FATF's black and grey lists, and revising the procedures for their formation in light of the newly-adopted mutual evaluation guidelines;
- continuing the work on the concept of the FATF expansion strategy;
- discussion of the early outcomes of a study into effectiveness of oversight activities and enforcement practices;
- fulfilling the priority goal of the Russian Presidency of the FATF relating to the detection of financial flows linked to Afghan drugs trafficking.

FATF member states approved the AML/CFT mutual evaluation procedures, drafted on the basis of the adopted in October 2013 procedures for holding the 4th round of mutual evaluations and applicable to all assessment bodies (FATF, FSRBs, IMF and World Bank). The impetus to draft the said document is connected with the need to create a global review mechanism that would be acceptable to the above institutions and that would enable the establishment of mutual evaluations quality standards and a common approach to their implementation.

As part of the FATF's on-going efforts to identify and monitor jurisdictions with strategic AML/CFT deficiencies that pose a threat to the global financial system, the Plenary participants once again updated the FATF's black and grey lists.

Following a review of the countries' progress in the implementation of national action plans to remedy the strategic AML/CFT deficiencies in the period since October 2013, Kenya and Tanzania exited the black list, thereby continuing the last year's trend for its reduction. This means that instead of fifteen countries (February 2013), it now contains eleven: Yemen, Indonesia, Iran, North Korea, Myanmar, Nigeria, Pakistan, Syria, Turkey, Ecuador and Ethiopia.

During the meeting of the International Cooperation Review Group (ICRG), the work to revise the group's procedures in light of the newly-adopted mutual evaluation guidelines, which began in June 2013, was continued. Among the topics attracting most interest were the discussion of the possibility of using a new version of recommendation 1 (Evaluation of ML/FT-related country risks) as one of the criteria for inclusion in the FATF's grey or black lists, the interconnection between the monitoring of jurisdictions' efforts to correct deficiencies after undergoing mutual evaluations and the application of more stringent ICRG procedures, as well as the introduction of possible changes to these procedures and the deadlines for their development and approval.

The Plenary also saw the defending of their follow-up reports by Australia, Austria, Argentina, Aruba, Iceland, Luxembourg, Mexico, the Netherlands, the USA, Turkey and Japan.

During a review of Turkey's follow-up report, participants pointed out the deficiencies still existing in respect of Special Recommendation III, in particular, the absence of the elements necessary for the implementation of an effective mechanism for freezing of terrorist assets.

In the course of the discussion of Kyrgyzstan's follow-up report dedicated to the elimination of strategic AML/CFT deficiencies, participants praised Kyrgyzstan for progress in implementing the majority of the requirements of its Action Plan, prepared jointly with the FATF, and voted in favor of sending to Kyrgyzstan a FATF verification mission to enable the subsequent removal of this country from the grey list.

Participants also noted the successful implementation by Tajikistan of the national AML/CFT action plan.

The Plenary extended the mandate of the FATF Expansion Task Force (hereinafter the «ETF», which includes Mexico, Canada, China, Russia, USA, France

and South Africa), established in February 2013, until June of this year, which is necessary to complete the development of the FATF strategy for admission of new members.

During the meeting of the Policy Development Group (PDG), participants heard the results of a survey of FATF and FSRB member states related to a study into effectiveness of oversight activities and enforcement practice, launched late last year. The survey findings were subsequently analyzed to identify the four main areas of further work on the topic:

- application of a risk-based approach to oversight activities;
- protection of banking secrecy and personal data;
- issues related to the efficient use of resources in the area connected with oversight activities and raising awareness among oversight agencies and accountable institutions of the requirements of domestic AML/CFT legislation and international standards;
- issues related to the effectiveness of enforcement practice.

It was decided that an appropriate document defining the direction of work in this area should be prepared by June.

One of the issues discussed during the Plenary was the effectiveness of application of FATF standards in respect of the procedures for the establishment of beneficial owners, as well as the work relating to the study of virtual currencies.

It is worth noting the consensus existing in the international community with regard to the growing popularity of virtual currencies (on February 6, 2014 Rosfinmonitoring released a statement titled «On the use of crypto-currencies,» noting that the use of crypto-currencies in transactions should be viewed as the grounds for classification of such transactions as operations linked to money laundering and terrorist financing). During the meeting of the Risks, Trends and Methods Working Group, participants held a discussion dedicated to this topic.

In the context of AML/CFT, bitcoins, gold, precious stones, works of art, etc. have much in common: they can be converted into local currency in just about every country. According to a generally held view, money-laundering transactions can be carried out using money or any other commodity. This fact was reflected

both in the FATF's and FSRBs' initiatives: in the recently released by the FATF guidance dedicated to money laundering and terrorist financing through gemstones, as well as in the joint EAG/APG study into the use of gold, etc. for ML/FT.

In the short term, work will be conducted in the following areas:

- monitoring of the new types of decentralized currencies;
- monitoring of countries' efforts in adopting new laws governing virtual currencies.

In addition, the plenary week saw the continuation of the work on the implementation of the FATF Russian Presidency initiatives concerning the detection and subsequent blocking of illicit financial flows from the production and trafficking of Afghan drugs. A regular meeting of the project group for the preparation of the corresponding typological study was held on the sidelines of the Plenary jointly with the UNODC.

Among other events held during the Plenary were meetings with co-chair of ICRG, deputy secretary of the U.S. Treasury D. Glaser, EAG Chairman K. P. Krishnan, deputy head of the Office for Combating Money Laundering of the People's Bank of China Liu Zhen Ming, executive secretary of the Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL) John Ringguth, as well as with the heads of financial intelligence units of Spain, Kazakhstan, Kyrgyzstan, Tajikistan, Turkmenistan and Uzbekistan.

Additionally, consultations were held with the heads of delegations of the EAG member-states dedicated to the topical issues of EAG management and the current situation with the reports on the progress of national AML/CFT systems ahead of the joint FATF-EAG Plenary, to be held in June of this year in Moscow.

MONEYVAL'S 43RD PLENARY MEETING

On 9-14 December 2013, Strasbourg (France) played host to the 43rd Plenary Meeting of the Committee of Experts on the Evaluation of Anti-Money Laundering and Financing of Terrorism (MONEYVAL), a FATF-style regional group

Nikita A. Bobryshev,
Project manager of Analysis and Information Department

One of the items on the agenda was elections to the MONEYVAL Bureau. A. Bartolo (Malta) retained the post of chairman, while D. Thelesklaf (Liechtenstein) was elected deputy chairman after coming out on top in a contest with other candidates. Among the newly elected members of the Bureau is Russia's A G. Petrenko, the head of International Cooperation Department of Rosfinmonitoring.

In September 2013, the Committee of Ministers of the Council of Europe approved amendments to MONEYVAL's Charter, granting the right to vote and the opportunity to participate in elections to the Bureau to Israel, the Holy See and the British Crown dependencies of Guernsey, Jersey and the Isle of Man (one vote for three jurisdictions). During the current 43th meeting, for the first time the voting was conducted with account of these members' votes.

Additional attention of the Plenary was devoted to the preparations for the 5th round of MONEYVAL mutual evaluations.

The Plenary reviewed the follow-up reports of Bosnia and Herzegovina, the Holy See, Hungary, Georgia, Moldova, Montenegro, the Czech Republic and the British Crown dependencies of Jersey and Guernsey. A mutual evaluation of Israel has shown that this country has made progress both with respect to key and core recommendations. Additionally, participants heard a special report prepared by Cyprus on the effectiveness of customer due diligence in banking.

Serbia presented a report on national risk assessment, which generated considerable interest among the delegations due to the upcoming new round of FATF mutual evaluations. Among the main problems encountered during the assessment were the lack of uniform statistical information from agencies (or its complete absence), difficulties with setting up working groups from representatives of relevant authorities (lack of coordination) and a shortage and low quality of ML-related materials. Based on the assessment results, the country has set up a working group and drafted a strategy for the development of Serbia's AML/CFT system for 2014-2019.

MONEYVAL's 44th Plenary meeting will be held in early April 2014.

REPRESENTATIVES OF U.S. AND EUROPEAN FINANCIAL INSTITUTIONS DISCUSSED THE FIGHT AGAINST MONEY LAUNDERING IN MIAMI

The annual conference of the Florida International Bankers Association (FIBA) is one of the biggest anti-money laundering and terrorist financing events in the U.S. and probably in the world

Viktor L. Dostov,
Chairman of the Electronic Money Association

Almost one thousand delegates from the United States, Latin America and other countries gather annually for two days in Miami to discuss a wide range of industry-specific issues. One important aspect of the gathering is the already customary presence at it of government officials; about fifty employees of the U.S. Treasury, the Financial Intelligence Unit, the FBI and other organizations make speeches, organize question-and-answer sessions and take an active part in ongoing discussions. The state-private sector engagement has traditionally been a strong element of the AML/CFT system, as well as being encouraged by the FATF and its regional bodies, which is the reason why it has been made the main theme of the conference.

The range of topics covered at the conference is broad, with much attention naturally being given to the general and topical issues of money laundering: identification of beneficial owners and politically exposed persons, as well as the new country-based risk guidelines, in conjunction with which the new FATF Recommendations will be implemented. Even greater emphasis, however, is devoted to regional specifics: issues related to the implementation of the FATCA by both the U.S. and, which is more important for us, foreign financial institutions, the activities of the Office of Foreign Assets Control (OFAC), and aspects of trade policies. Such a wide scope is explained by the evolution of AML/CFT activities. If at the end

of the 1980s, for example, the fight against money laundering was primarily directed at the proceeds from the sale of drugs, today it includes measures against tax evasion, the proliferation of weapons of mass destruction, corruption and many other public hazards.

FIBA (Florida International Bankers Association) – is a non-profit trade association. Its membership includes more than 70 banks in the U.S. and beyond. The primary business focus of FIBA is to strengthen financial ties with Latin America. In addition to interacting with regulators in the countries concerned, the association arranges a number of special events, with the annual AML/CFT compliance conference in Miami, which attracts more than 1300 representatives of the largest U.S. and European financial institutions, being one of them. As a trade association, FIBA also conducts AML/CFT trainings and certification of financial institutions' employees.

Rather interesting is the experience of the U.S. in setting up an AML/CFT regime in the context of strong federalization principals, where anti-money laundering requirements and other regulations may vary from state to state. In particular, it raised a curious, yet secondary question: how can banks work with marijuana venders if the head office of the credit institution is located outside the state where the sale of cannabis is legalized?

As a result, discussions taking place at the FIBA conference touch upon a wide range of issues, from general to highly technical. The full program of the conference can be found on the official website of the event. Still, some of the topics raised by the organizers deserve special mention.

First, it was interesting to see how much time was devoted to the clarification of issues concerning the private sector by government agencies. Regulators described in detail the purpose of the measures companies are legally required to undertake, and explained how the collected by financial institutions data is used for solving real crimes.

Another group of issues discussed at the conference was devoted to the evolution of law enforcement, to which was also dedicated a large part of a report by director of the U.S. financial intelligence unit Mrs. Jennifer Shasky Calvery. As noted above, supervisory bodies maintain rather effective communication with the private sector on regulatory issues, but, in our opinion, they often do not do enough to explain their objectives and working methods. This conference is a pleasant exception. Over the past decade and a half, international practice, as well as the policies of individual states, has come a long way. Right before our eyes, countries are rapidly moving away from the formal approach and increasingly focusing on efficiency and deep information analysis. The better

financial institutions understand the principles that form the basis of this work, the more relevant the data reported by them will become.

The second group of issues, which the author found particularly noteworthy from a professional point of view, was devoted to the fastest growing segment of the AML/CFT cluster: technological challenges facing the fight against money laundering. This group included topics ranging from risks associated with new payment methods to such a hot topic as decentralized cryptocurrencies. Experts also exchanged views on the issue of cybercrime, a new, but unfortunately, fast-growing type of predicate offenses. Representatives of the Electronic Money Association traditionally act as experts on this subject, including this year when they took part in a large panel discussion on virtual currencies. Despite the fact that the experience of each jurisdiction in relation to new financial phenomena is unique, representatives of the public and private sectors expressed their support for a flexible, moderate approach as opposed to restrictive measures. Apparently, this is the only way to ensure effectiveness of intelligence activities without jeopardizing innovation.

The third group of issues, which is almost completely ignored in Russia and other countries, was discussed at the workshop titled «Getting started – development of an AML/CFT program after application of regulatory sanctions». Participants discussed in detail the issue of restructuring of internal control programs of the credit institutions subjected to severe penalties for AML/CFT violations. In Russia, the range of such sanctions is, unfortunately, extremely limited: either a moderate administrative penalty or revocation of a license. Although a bank closure puts an end to

OFAC (Office of Foreign Assets Control) – of the U.S. Treasury Department is responsible for enforcing economic and trade sanctions based on U.S. law and international agreements (including UN sanctions). OFAC updates the sanctions lists in the areas related to combating terrorism, drug trafficking and proliferation of weapons of mass destruction. A separate category of sanctions is designed to apply to jurisdictions: Iran, Syria, Cuba, North Korea, etc. Particular interest is devoted to targeted sanctions: in recent years they have been used against officials from Belarus, Burma, Lebanon, Libya and some other countries.

U.S. financial institutions are required to freeze the assets of individuals and entities included in the sanctions lists, refuse to execute transactions ordered by such persons, and notify OFAC. Given that Russian banks can use correspondent accounts in the U.S., OFAC requirements indirectly apply to them, too. There have been instances when funds belonging to the customers of Russian banks in foreign correspondent accounts were frozen for violations of the sanctions regime.

illegal transaction, it also inevitably adversely affects legitimate customers who are not responsible for bad management practices. Perhaps, special rehabilitation programs in the field of AML/CFT would be no less useful than measures for financial recovery problematic credit institutions.

Events like the annual FIBA conference are useful because they allow us to look the challenges facing us from a wider angle. Although different countries face different challenges, experts are gradually coming to an opinion that solutions are mostly universal. Many of them have already been described by the FATF: it is important to accelerate transition to a risk-based approach and introduce regulatory measures based on an analytical approach to information gathering.

Apparently, these are the areas that will determine the further development of the AML/CFT regime globally.

TREND

ALTERNATIVE CURRENCIES: DIVERGENT TRENDS IN THE DEVELOPMENT OF THE "NEWEST" PAYMENT METHODS

The sheer volume of data existing in the world today is truly overwhelming; so much so that even the world's most powerful supercomputers will probably never be able to systematize and organize all the information available online into a medium understandable to average Internet users. At the dawn of the Internet age, computers were a lot less common than in today's world, where each user typically owns multiple gadgets (e.g., a tablet computer and a mobile phone, in addition to a desktop PC) connected to the Internet. Also on the rise are user numbers, driven by the increasing availability of wireless technologies for data delivery and access

Konstantin G. Sorokin,
Columnist, PhD

According to some experts, in 2010 for the first time in history there was more than one Internet-connected device per each living person (the number of such devices reached 12.5 billion last year, while the world's population stood at 6.8 billion)[1]. A group of Chinese researchers analyzed the Internet traffic growth rate over the period from December 2001 to December 2006 at 6-month intervals, concluding that, by analogy with Moore's Law, Internet traffic doubles every 5.32 years[2]. In 2008, the world generated about 5 exabytes of unique data, enough to fill 1 billion DVDs. And only three years later, the volume of unique data reached 1.2 zettabytes. Interestingly, to create a

[1] http://www.cisco.com/web/RU/news/releases/txt/2011/100411.html

[2] http://www.cisco.com/web/RU/news/releases/txt/2012/012012c.html

similar volume of data in Twitter, every inhabitant of the Earth would have had to tweet nonstop for 100 years, or, for comparison, an equivalent of 250 billion DVDs[3]. According to some studies[4], up until the start of twentieth century the volume of accumulated knowledge doubled every 100 years. Today, however, the total volume of human knowledge doubles every two or three years, thanks in no small part to the Internet, which is responsible for about 70% of all data – and counting[5]. According to Cisco System report, since 2007 to 2012 every two year there was doubling of IP-traffic in the world of IP - networks[6].

Such rapid development of information technology is responsible for another interesting trend: many countries that struggled to finance the development traditional landline infrastructure for Internet access are now skipping this stage altogether and moving on to wireless access, primarily through mobile devices, thereby contributing to the growth of potential and actual Internet users.

In addition to rising volumes and coverage, another key trend is the speed of information dissemination. For example, messages from the Japanese Twitter users about the earthquake showed up on the social network even before the U.S. seismic authority issued its first tsunami warning to the residents of Alaska, Washington, Oregon and California[7]. Such changes have become possible thanks to the mobile Internet and users' ability to generate content anywhere at any time. In essence, it means that every smartphone owner will soon be able to generate and disseminate data in real time[8].

Among the sectors affected by these or similar trends is the world of finance. Even though e-money,

[3] http://www.cisco.com/web/RU/news/releases/txt/2011/100411.html

[4] http://www.cisco.com/web/RU/news/releases/txt/2012/012012c.html

[5] http://www.cisco.com/web/RU/news/releases/txt/2012/012012c.html

[6] http://www.opennet.ru/opennews/art.shtml?num=16549

[7] http://www.cisco.com/web/RU/news/releases/txt/2011/100411.html

[8] http://www.cisco.com/web/RU/news/releases/txt/2011/100411.html

which only recently was viewed as the so-called «new» payment method, has by now made it into our daily lives, the properties of some of the «newest» payment methods, including cryptocurrencies (altcoins[9]) have taken us by surprise; in essence, we are talking here about an alternative to both gold, as a timeless value, and to instant money transfers which are not regulated. And if the «new» payment methods, which have already become almost traditional, are subject to some forms of regulation, the «newest» are still beyond it.

For example, it is only by using the «newest» payment methods that any given person may wire transfer, say, several hundreds of millions of dollars on the New Year's Eve, when all banks are closed, to a high-risk in terms of ML/FT country (e.g. Afghanistan) almost in real time, and, to top it all, enjoy the guaranteed protection against any transaction freezing measures that may be attempted by any regulator. What is even more unusual is that such a transaction can even be carried out without any direct connection to the Internet, e.g. by linking together two laptops, or even via satellite communications (the updating of digital wallets will occur during the nearest online session). Another interesting trend worth mentioning and which has the potential to surprise those experts who refer to cryptocurrencies as speculative instruments concerns the limited use of the most popular type of altcoins – Bitcoin, only about 25% of the issued altcoins of this type[10] enter circulation (i.e. used in transactions). The remaining three-quarters of these instruments remain outside the electronic transfer system, and may either change hands together with the storage medium containing the digital wallet during a physical contact between two persons, or stay away from electronic trading for other reasons (loss of the digital wallet access codes, use as a saving instrument, etc.), highlighting the risks associated with such use.

Along with the growing popularity of the «*new*» and «*newest*» *online payment systems*[11], Internet users have become increasingly fascinated with the phenomena called *crowdfunding*[12] – the collection of finance to sustain an initiative from a large pool of backers – the «crowd» – usually made online by means of a web platform. The initiative may have different goals. e.g. assistance to victims of natural disasters, fans' support for their team, support for political campaigns, financing start-up companies, creation of free software, generating profit from joint ventures, etc. Crowdfunding, however, may also be used to raise funds for less honorable causes.And when coupled with the opportunities created by the «newest» payment systems – especially altcoins – and the diversity of legislative frameworks existing in different jurisdictions (when fundraising activities are regarded as an offence in one jurisdiction but are perfectly legal in another), it becomes clear that such payments may pose a real danger to society. Exercising the proper control over such transactions, on the other hand, may be difficult given the transnational nature of such payments. And although authorities in Russia, unlike western countries, have until now been able to identify isolated cases of crowdfunding in support of illegitimate initiatives, sooner or later they will be confronted with this phenomenon on a massive scale. This will be primarily due to the ever-increasing numbers of new initiatives and users participating in them as a consequence of Moore's Law[13], as well as the pressing need to identify the most dangerous initiatives. Altcoins are perfect for this type of activity: no intermediaries, no commissions and no extra costs.

With regard to charity, the use of altcoins-based crowdfunding schemes can give almost 100 percent guarantee that every electronic donation will reach the person in need, as proponents of the charitable use of bitcoins in Uganda[14], a country where donations often go astray, can attest. The main problem here lies in providing recipients with access to the required technology, whereas, given the opportunities offered

[9] Some experts assign altcoins (alternate cryptocurrencies) to the category of alternative (or replacement) currencies, including Bitcoin. However, others believe that altcoins fall into a category of cryptocurrencies that are alternative to bitcoins and that do not include Bitcoin itself. See a list of the top 100 cryptocurrencies at http://coinmarketcap.com. The author also recommends to view the description of cryptocurrencies at http://altcoins.com

[10] http://hr.superjob.ru/raznoe/bitcoin-i-drugie-kriptovalyuty-traektoriya-uspeha-s-alekseem-porhunovym-dengi-buduschego-i-ih-hozyaeva-712?utm_source=email&utm_medium=email&utm_campaign=news-subscriptions.

[11] The author uses the term «newest payment methods» to describe payment methods, including altcoins, that are relatively new and not subject to any specific legal regulation. Most of them, but not all, are connected with information technologies.

[12] http://ru.wikipedia.org/wiki/%D0%9A%D1%80%D0%B0%D1%83%D0%B4%D1%84%D0%B0%D0%BD%D0%B4%D0%B8%D0%BD%D0%B3

[13] Moore's Law http://ru.wikipedia.org/wiki/%D0%97%D0%B0%D0%BA%D0%BE%D0%BD_%D0%9C%D1%83%D1%80%D0%B0

[14] Http://russian.rt.com/article/18166

by wireless Internet access, the potential to expand such access is evident. Meanwhile, the role played by charities in this case may be slightly adjusted to include, among others, the provision of access tools, training and fund allocation. At the same time, the success of this system will depend on the availability of the relevant infrastructure (receipt and issuance of altcoins), whose lack will act as a drag on the proliferation of these technologies, at least in the short term.

At the same time, the use of new technologies in the financial industry, albeit to achieve slightly different goals, has already seen practical application in some third world countries. One such country is the Democratic Republic of Congo, where authorities made a financial «revolution» in the first half of 2013 by introducing an electronic payroll system for civil servants[15]. A comprehensive switch to the so-called «mobile banking», which is quite common in developed countries, was highly unusual for Congo, where until recently most transactions had been carried out in cash. Moreover, the DRC government institutions had a tradition whereby officials received their wages from the hands of their immediate boss, a practice that contributed to corruption. As a justification for avoidance of electronic payments, authorities cited various «operating, transportation and other overhead costs.» In the army, for example, soldiers used to be paid in cash only about 5% of their $100 salaries. Following the introduction of the new system, civil servants are no longer subject to intrusive and burdensome intermediary services, while their wages are now credited directly to their personal bank accounts, of which they are notified by SMS[16]. Because towns and villages in the DRC are scattered over a huge and often poorly accessible territory, the country does not have an extensive network of bank branches. Equally inadequate is the accessibility of financial service to the public. With an average per capita income of about $200, only 2 percent of the population had access to financial services in 2012[17]. The introduction of new services allowed the government to pay wages to civil servants in large cities directly to their bank accounts, with rural inhabits still collecting their salaries in cash from the local office of a mobile operator.

The introduction of new services has benefited the authorities too, resulting in the disappearance of nonexistent – on-paper-only – civil servants whose wages ended up in the pockets of corrupt officials. It is possible that altcoins may also become popular in some developed countries, while the supporting infrastructure may, as in the above example, come from other industries (e.g. mobile operators who are keen to increase their customer base by offering mobile Internet services). The U.S. Postal Service, for example, is seriously considering the opportunity to improve its finances by offering exchange services for cryptocurrencies in a move prompted by reduced customer traffic and falling business volumes, as well as by the need to maintain its network and find new ways to fill its offices. One potential point of contact is a virtual currency exchange service[18]. The move is made even easier by the fact that many postal operators already offer financial services, i.e. money transfers, payment of bills, etc., and, therefore, have all the necessary licenses and permits. The U.S. Postal Service, for one, owns a money transmitter license, allowing it to offer cryptocurrency exchange services in all of its 36,000 branches[19].

Given the low cost of cryptocurrency transactions, one may expect them to challenge the dominance of traditional money transfers, including by capturing such important sector as migrant remittances. It is also quite possible that even the largest money transfer operators may, when faced with the threat of losing

[15] Http://eterra.info/mosaic/allo-zarplata-slushaet

[16] Http://eterra.info/mosaic/allo-zarplata-slushaet

[17] Http://eterra.info/mosaic/allo-zarplata-slushaet

[18] Http://cryptorise.info/news/us-post-bitcoin-exchange

[19] Http://cryptorise.info/news/fincen-mining

market share, choose to jump on the bandwagon and try to cash in on the currency exchange rate difference between the sender's and recipient's country, rather than trying to resist the arrival of altcoins. Thus, we can expect the development of the infrastructure needed to handle virtual currencies to take place through mobile operators, postal services, etc. Interestingly, the company that produced the first Bitcoin ATM in Canada also created an ATM for another digital currency – Dogecoin[20]. In his interview with The Georgia Straight newspaper journalist Stephen Hui, Warren Jackson, one of the creators of cryptocurrency ITMs, said that his company Bitcoiniacs is now working to produce mini ATMs costing less than $1,000[21]. Accordingly, the problem of infrastructure development will, sooner or later, be solved, with only the form (or a combination of forms) of the solution still undecided.

Therefore, despite some infrastructure-related challenges, further expansion of cryptocurrencies into the charitable sector, especially crowdfunding, seems all but inevitable. And if we take into account the trend towards globalization, it will become clear that projects related to the collection and distribution of such currencies can be implemented anywhere in the world, making the task of law enforcement agencies monitoring and identifying risky transactions ever more difficult. For comparison, already now some Internet communities are actively accepting donations in cryptocurrencies to finance a variety of projects. For example[22], the Dogecoin community on Reddit is raising funds for research. Experiment.com, on the other hand, offers independent researchers and philanthropists a meeting place where to unveil new research projects and specify their budget requirements. It took one community on Reddit only one day to raise 300,000 dogecoins[23] for three projects: West Virginia Chemical Spill Research, Patterns and Effects of American Crow Movements, and Leatherback Sea Turtle Research.

Law enforcement authorities are bound to come across numerous initiatives that have nothing illegal about them, as well as some initiatives that do not pose a direct threat to the public, e.g. raising funds for causes

that are somewhat different from those stated officially (the ultimate goal of such fundraising campaign is to enrich a specific fundraiser by committing, as is in this case, a fraud). Sifting through such initiatives manually will take way too long, making the challenge of identifying particularly dangerous cases in a vast array of information particularly daunting.

Whereas a huge number of alternative currencies (altcoins) coupled with the possibility of their mutual conversion will only add to that challenge. It is no secret that special agencies have, ever since the time of the famous signals intelligence collection system Echelon[24] and related projects, been handling vast amounts of highly diverse intelligence. However, if in the past the emphasis was on intelligence access and interception, today it is increasingly on its analysis, selection and interpretation. Additionally, the online fundraising activities of some individuals or groups of individuals are not conspiratorial in nature, but rather designed to appeal to the widest possible community of people who may act as potential donors. Thus, the focus of such agencies' efforts should be on the detection of a small number of illegitimate fundraising initiatives and on monitoring transactions in altcoins, taking into account the transnational nature of some of these transactions and their potential for avoiding real time network detection.

[20] Http://cryptorise.info/news/wow-dogecoin-atm

[21] Http://cryptorise.info/news/wow-dogecoin-atm

[22] Http://cryptorise.info/news/dogecoin-nauka-experiment

[23] For more info on the currency exchange rate, please visit http://bitinfocharts.com/ru/dogecoin, 1 dogecoin equals $ 0.0012 as of Feb. 22, 2014.

[24] Http://ru.wikipedia.org/wiki/%D0%AD%D1%88%D0%B5%D0%BB%D0%BE%D0%BD_(%D1%81%D0%B5%D0%BA%D1%80%D0%B5%D1%82%D0%BD%D0%B0%D1%8F_%D1%81%D0%BB%D1%83%D0%B6%D0%B1%D0%B0)

In addition, it is time for special agencies to start allocating funds in their budgets to cover the cost of social networks and Internet monitoring and identifying such activities, taking into account the projected rate of growth and development of these trends. That said, it is important to remember that when it comes to processing data, the activities of law enforcement authorities of almost all countries are subject to, in one form or another, the economic cost-effectiveness criteria. In light of the challenges facing the global economy, many countries have unofficially abandoned the policy of thorough transaction processing and investigations in cases where their cost is projected to be higher than the expected economic effect. Already now the scientific and educational community (especially the legal sector and IT) should start looking for ways to integrate the «new « and «newest « payment methods, bearing in mind, among others, their transnational nature and inherent properties, into the existing legislative framework in order to allow their regulation and curtailment of the threats posed by them, and to carry out a mandatory, cost-effective monitoring of such transactions (most of which are beyond the scope of reporting entities or mandatory supervision) and related fundraising initiatives for the benefit of law enforcement, special agencies and supervisory authorities.

And if we think more long term, then, there should be special IT courses devoted to this subject, whose graduates will combine the legal aspects of the problem and the practical experience of using the «new» and «newest» payment methods (including altcoins), while, and this is particularly important, placing a special emphasis on AML/CFT.

U.S. FOREIGN ACCOUNT TAX COMPLIANCE ACT (FATCA)

The Foreign Account Tax Compliance Act (FATCA) entered into force on January 1, 2013 and will become binding starting from July 1, 2014. The FATCA main objective is to prevent tax evasion by U.S. individuals and legal entities

Inessa A. Lisina,
editor and correspondent

At one of the recent sessions of the U.S. Congress, it was announced that tax avoidance schemes operated both through offshore and different foreign jurisdictions cost the U.S. about 100 billion a year. It should be noted that the U.S. tax law requires its citizens to pay taxes irrespective of their residence, location of their property, business or income source.

It is the fight against tax evasion that the new tax regime is intended to lead. Initially the FATCA was expected to take effect already on January 2014. However, the U.S. eventually had to move that date forward to July 1, 2014 in order to give some countries more time to align their position with that of the U.S.

The act requires banks and financial institutions around the world to report to the U.S. Internal Revenue Service all transactions carried out by their American clients.

U.S. citizens proof of identification:

1. U.S. passport
2. U.S. place of birth
3. U.S. citizenship
4. green card
5. one U.S. citizen parent (provided he or she has lived in the U.S. for at least 5 years after reaching the age of 14).

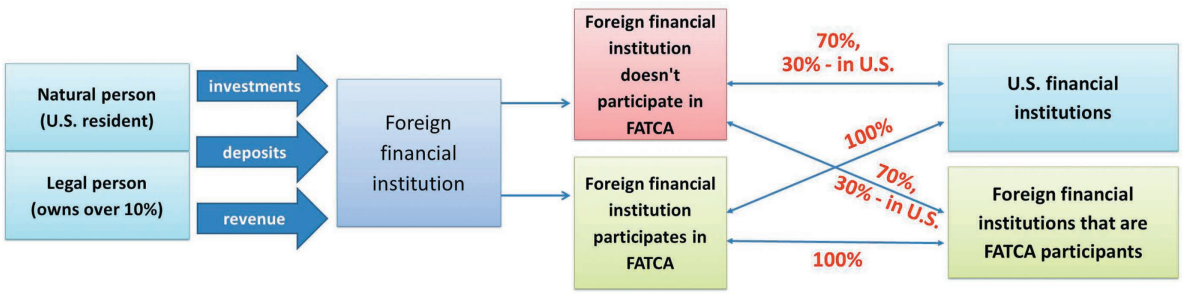
There are several ways in which this tax regime can be implemented in practice. The first provides for conclusion of agreements between the U.S. and foreign countries. In this case, financial institutions will provide information about U.S. accounts to the tax authorities of their country, which, in turn, will forward it once a year to the U.S. Internal Revenue Service. Engagement here can also be carried out two ways: such an agreement may involve mutual information exchange (the U.S. will share information about the partner country's taxpayers with the partner country), or an arrangement under which the information will be sent only to the U.S. (a non-reciprocal model).

Currently there are more than 20 countries that have already signed intergovernmental agreements with the U.S., among them are the United Kingdom, France, Germany, Italy and Spain. All the financial institutions of these countries have to do now is simply to register with the U.S. Internal Revenue Service, which can be done on the agency's website or by mail.

The second option provides that if, for whatever reasons, the U.S. fails to reach an agreement with a foreign country on information sharing within the FATCA regime, then financial institutions of that country may report directly to the U.S. Internal Revenue Service. To do this, they also need to register with the U.S. Internal Revenue Service until July 1, 2014 and get a registration number.

Japan and Switzerland went down a different path, though. They have signed intergovernmental agreements with the U.S., under which their financial institutions will submit information on U.S. accounts directly to the Internal Revenue Service, bypassing the national tax authority.

Fig. 1: Interaction process during the use of EPT



Information that banks and financial institutions will provide to the U.S. Internal Revenue Service (or to the tax authority of their country):

- U.S. natural or legal person's name, address and TIN
- Their account numbers
- Accounts' balances, receipts, and withdrawals

There can be no doubt that the FATCA regime requirements have a directly impact on domestic laws on the protection of banking secrecy and account information, leading many banks and financial institutors to express concern about the possible implications of its enactment. However, it is virtually impossible to avoid the effects of the new tax regime, given that it provides for severe consequences in the form of a 30% withholding on all international money transfers for any country or financial institution that fails to sign either an intergovernmental or its own agreement on joining the FATCA regime. That said, the withholding penalty will be levied not only on money transfers going through the U.S., but also via the countries that have joined the FATCA. All U.S. banks have already received detailed instructions on withholding requirements from the national government. Therefore, in order to avoid potential losses, banks will have no other choice but to join the new U.S. tax regime.

The Russian government has decided to sign an intergovernmental agreement with the U.S. on mutual exchange of information on taxpayers. The document is expected to be signed by July 2014 to enable Russian banks to avoid possible sanctions.

According to the draft regulation, the Russian banks will provide information about U.S. accounts through the Federal Tax Service, while U.S. authorities will assume the obligation to share data on Russian accounts in the U.S. with Russia.

In which cases are banks and other financial institutions required to provide information on the accounts of U.S. entities and individuals?

If the account balance reaches a specified threshold ($50,000 for individuals and $250,000 for legal entities), such account becomes subject to the FATCA requirements. With regard to legal entities, however, information must be provided only if U.S. residents directly or indirectly own 10% of that amount.

As we can see, the purpose of the FATCA act is not only to increase revenues and taxes collected by the U.S. Treasury, but also to combat illegal financial transactions worldwide. Insuring compliance with the FATCA requirements will require financial institutions around the world to reevaluate the effectiveness of their «know your customer» procedures and ensure compliance with the ant-money laundering and terrorist financing requirements, as well as possibly revise and amend the procedures for opening new customer accounts and recording of transactions carried out through them.

Despite all the challenges associational with the implementation and operation of such a tax regime, several major political actors have already appreciated the global effect the FATCA will have on the international market of finance and remittances. Similar tax regime initiatives are expected to be developed and implemented by the European Union and the Organization for Economic Cooperation and Development. We will be in a position to judge the effectiveness of these tax regimes only some time after their introduction. Despite this, already now we can talk about tightening of controls over financial transactions worldwide.

EDUCATION AND SCIENCE IN AML/CFT

ROUNDTABLE DISCUSSION "TAX CRIMES AS MONEY LAUNDERING PREDICATE OFFENCES"

Discussion Of The Results Of ITMCFM's Research Titled "Tax Crimes As Money Laundering Predicate Offences: Approaches To The Implementation Of International Standards"

Konstantin G. Sorokin,
columnist, PhD

During a roundtable discussion with the EAG countries organized by the ITMCFM via videoconferencing, participants examined the issue of recognition of tax crimes as money laundering predicate offences. The event was attended by representatives of the FIUs, law enforcement and other government authorities of Belarus, Kazakhstan, Tajikistan and Uzbekistan.

Among others, Russia was also represented at the roundtable by employees of the Research Institute of the Academy of Prosecutor General of Russia. The relevance of this topic for Russia is underscored by the fact that Russia only recently added tax crimes to the list of money laundering predicate offences, as required by the FATF international standards.

Among the issues discussed during the meeting were:

- whether the criminal law permits the recognition of tax crimes as predicate for money laundering;
- if it becomes a law, is there any judicial practice in this area. What challenges does it pose to law enforcers;
- how is the criminal income from a tax crime determined, and how does it relate to the subject of a money laundering offence;
- is it necessary to identify the specific property that has been obtained illegally as a result of a tax crime, or it is enough to just establish the fact of tax evasion and concealment of the criminal origin of illegal income through financial and other transactions with any property of the taxpayer;

- can a money laundering offence occur at the time of preparation or attempt to commit a tax crime;
- if the criminal law does not allow tax crimes to be recognized as predicate for money laundering, what are the prospects for the introduction of this kind of liability.

Participants also discussed the findings of a survey of member countries and the specifics of law enforcement.

Following the discussion, the parties acknowledged the relevance of the discussed issues and called for additional meetings to be held via videoconferencing in the future.

DOORS OPEN DAY AT THE ITMCFM

On February 24, 2014, the traditional annual doors open day was held at International Training and Methodology Center for Financial Monitoring (ITMCFM). Taking part in the event were the students and professors from the Institute of Financial and Economic Security, the senior managers of the ITMCFM and also the representatives of the FIUs of the EAG-member states (Belarus, Kazakhstan and Tajikistan) who participated in the meeting through the video conferencing mode

Alina V. Pascal,
Editor-columnist

The purpose of the meeting was to inform the students and the representatives of the FIUs about the main areas of activities of the ITMCFM and its structural departments, to present the *Financial Security* journal and the *Methodology for Assessing Technical Compliance with the FATF Recommendations the Effectiveness of AML/CFT Systems* on-line training course (which are the important projects implemented by the ITMCFM) and to brief the countries on the outcomes of the recent session.

In his welcoming address, Mr. Vladimir V. Ovchinnikov, General Director of the ITMCFM, pointed out that the graduates of the Institute of Financial and Economic Security are recognized as the highly qualified specialists and successfully and fruitfully work in the financial intelligence units of their respective countries: "*Using this opportunity, I request the representatives of the FIUs of the EAG member-states to pay special attention to education of their prospective students to make it easier for them to receive the training. And our task is to arrange for their proper training to avoid expulsion of the students which would be morally painful for them. Besides that, on-the-job-training in the national FIUs is arranged for ensuring further successful employment of the graduates. I wish good luck to all of us.*"

The ITMCFM General Director informed about the structural changes in the Center caused, inter alia, by the need to support the Russian Presidency of the FATF. At present, the office of the FATF President is held by Mr. Vladimir Nechaev, the First Deputy Director of the ITMCFM. The heads of the key departments

of the ITMCFM - Mr. Schekotikhin (Analysis and Information Department), Mr. Ivanov (Education and Science Department) and Mr. Ramishvili (International Cooperation Department) briefed the attendees on the priorities of their respective departments at the current stage of the development of the national AML system. Mr. Sorokin, the Advisor to the Education and Science Department, who acted in the capacity of the meeting moderator, presented the online assessors training course developed by the Center under the license agreement with the FATF, and Mr. Litvinov, the Deputy Chief Editor of the Financial Security journal, presented the main topics covered by the Rosfinmonitoring's periodical and encouraged the students to provide information and materials for publication.

In his presentation, Mr. Loskutov, the Deputy Director of the Institute of Financial and Economic Security and the officer of Rosfinmonitoring Human Resources Department, pointed out that the graduates of the Institute currently hold the core analytical job positions in Rosfinmonitoring: "*The graduates of the Institute of Financial and Economic Security have already accounted for 15% of the staff of the Rosfinmonitoring headquarters. In 2013, we accepted over one hundred students for on-the-job-training. Our employees who work as the trainers in the Institute teach and interact with the students on a daily basis, which, probably, plays the key role in training of highly qualified experts and specialists.*"

In course of further discussions, the participants paid special attention to the process of acceptance of prospective students for studying in MEPhI in 2014.

The participants from the EAG member-states countries noted the keen interest constantly paid by the FIUs of the EAG member-states in the projects implemented by the Center and supported further strengthening and extension of cooperation and coordination.

The event ended up with the special tour of the Center that was arranged for the students, in course of which they were provided with the opportunity to have informal discussions with the ITMCFM personnel.

ITMCFM EXPANDS ITS PARTNER BASE

Anna V. Bulaeva,
coordinator of the Education and Science Department of the ITMCFM

New challenges and threats to Russia's national security place greater responsibility not only on employees of organizations undertaking anti-money laundering and counter-terrorist financing activities (AML/CFT), but also on those responsible for AML/CFT training. Trainings take place in the form of introductory, supplementary and targeted briefings, as well as advanced AML/CFT courses.

The Targeted Briefing under the program titled «Combating money laundering and terrorist financing in organizations carrying out transactions with monetary funds and other assets» is provided to facilitate the development in the Russian Federation of a system for the training of employees of organizations carrying out transactions with monetary funds and other assets.

The AML/CFT Targeted Briefing is mandatory for the employees of organizations carrying out transactions with monetary funds and other assets. A list of such organizations is provided in Article 5 of Federal Law No. 115 of August 7, 2001 «On combating money laundering and terrorist financing.»

Under the existing Russian laws, the following categories of employees are required to undergo the AML/CFT Targeted Briefing at least once:

- head of the organization (branch);
- deputy head of the organization (branch) in charge of internal AML/CFT supervision;
- designated official of the organization (branch);
- chief accountant (accountant) of the organization (branch) (if any), or an employee in charge of accounting;
- head of the legal department of the organization (branch) or the organization lawyer (if any);
- employees of the internal control unit of the organization (branch) (if any);
- other employees of the organization (branch) designated by the head of the organization based on the organization (branch) and its customers specifics.

The AML/CFT Targeted Briefing is held at the International Training and Methodology Center for Financial Monitoring (hereinafter the «ITMCFM») once a month. The training takes place in the evening (18:30 to 21:45), lasts two days and is conducted with the involvement of Rosfinmonitoring's leading experts as well as executive secretary of the Eurasian Group on Combating Money Laundering and Financing of Terrorism Boris Toropov.

The AML/CFT Targeted Briefing is conducted in accordance with Federal Law No. 115-FZ of August 7, 2001 «On combating money laundering and terrorist

Audience during the AML/CFT Targeted Briefing held in the ITMCFM conference hall, January 28, 2014

financing» and Rosfinmonitoring Decree No. 203 of August 3, 2010 «On approval of the regulations concerning the requirements for the training of employees of organizations carrying out transactions with monetary funds and other assets in combating money laundering and terrorist financing.»

The main purpose of the AML/CFT Targeted Briefing is to help employees of organizations acquire up-to-date basic knowledge necessary for compliance with the Russian AML/CFT legislation, formation and upgrading of the system of internal controls of organizations, programs for its implementation and other organizational and administrative documents adopted for these purposes.

The main objectives of the AML/CFT Targeted Briefing are:

- to provide training to officials of organizations carrying out transactions with monetary funds and other assets responsible for internal controls and programs for its implementation;
- to facilitate the use by employees of organizations of uniform standards for application of legislative requirements;
- to raise the level of employees' AML/CFT-related professional skills and knowledge;
- to study the pattern of typical money laundering and terrorist financing schemes;
- to summarize and disseminate positive experience of organizations in establishing internal controls.

Attendees who have completed the AML/CFT Targeted Briefing and passed exams are issued with a standard certificate of completion, showing that they have completed an eight-academic-hour course.

Besides the ITMCFM, the AML/CFT Targeted Briefing is offered by educational and scientific organizations that have concluded cooperation agreements with the ITMCFM (hereinafter «ITMCFM partners»). The Center's partners conduct their activities in virtually all federal districts of the Russian Federation.

The goals of cooperation between the ITMCFM and its regional partners are:

- to establish a system for provision of AML/CFT training to employees of organizations carrying out transactions with monetary funds and other assets;
- to implement programs based on the AML/CFT Targeted Briefing;
- to set up a centralized registration system of graduates.

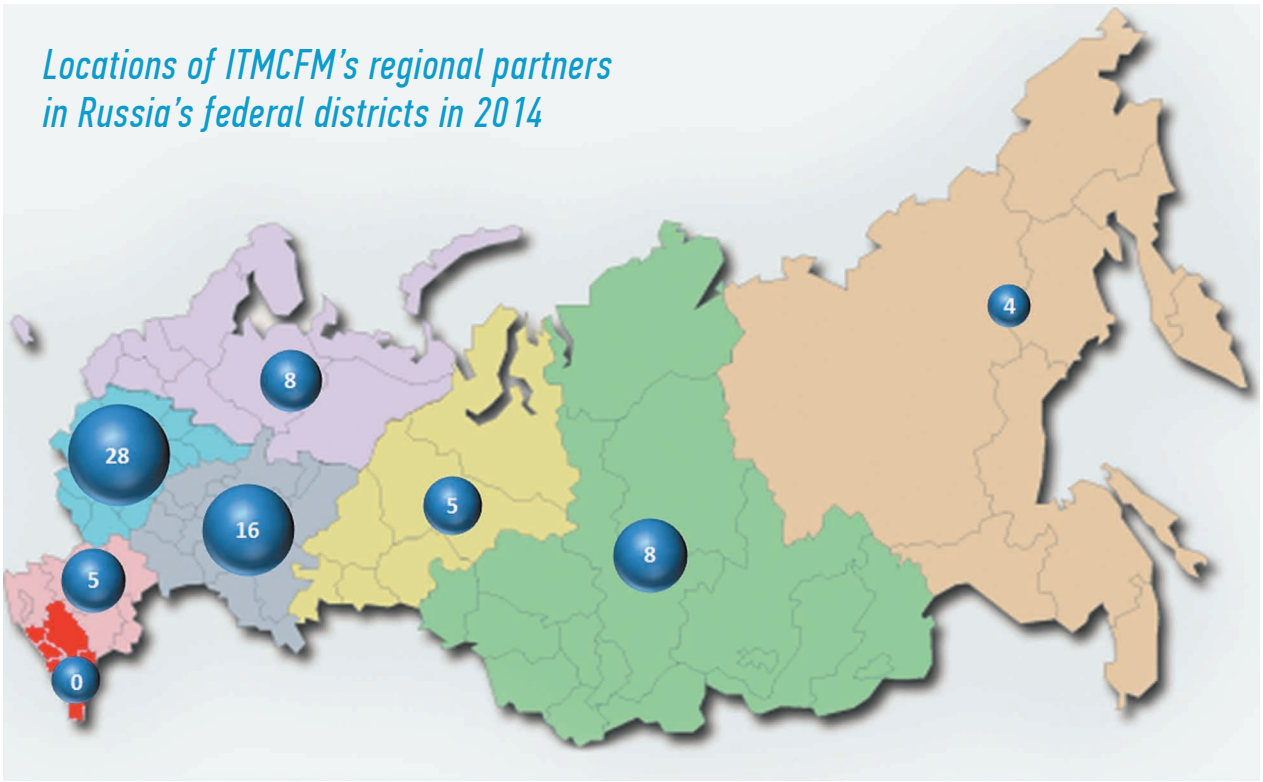
As of March 1, 2014, licenses to conduct AML/CFT Targeted Briefings were issued to 74 regional partners (77 in 2013, 72 in 2012 and 63 in 2011).

The national system for provision of AML/CFT Targeted Briefing-based trainings has a capacity to handle more than 13,000 students a year. Over the past five years, it has trained more than 50,000 persons.

The ITMCFM maintains a register of all issued AML/CFT Targeted Briefing certificates and a central register of persons trained. This information is used by the Federal Financial Monitoring Service for verification activities.

Currently, the ITMCFM is working to expand the number of its partners. The involvement in the teaching process of new members will increase the level of compliance with international requirements and reduce AML/CFT risks.

Locations of ITMCFM's regional partners in Russia's federal districts in 2014



EXPERTS ARE READY FOR EVALUATIONS

Inessa A. Lisina,
Editor and correspondent

On 10-14 March 2014, the EAG Secretariat jointly with the International Training Center for Financial Monitoring hosted a workshop for FATF and FSRBs (EAG/MONEYVAL/MENAFATF) experts dedicated to the preparations for a new round of mutual evaluations of national AML/CFT systems. The previous, third, round of evaluations took place from 2005 to 2010. Since that time, the FATF has revised its standards and drafted a new evaluation methodology.

The purpose of the FATF's on-site evaluation visits is to monitor compliance by the member-states with the FATF Recommendations and to assess its results. The new evaluation methodology provides for the analysis of two key criteria: technical compliance and effectiveness. The results awarded to the country following its mutual evaluation will affect the type of the monitoring process this country will be subject to, underscoring the importance of having enough highly qualified appraisers capable of executing such an important task. This methodology is used by all FATF-style regional groups, and for this reason among the priorities outlined by the elected in November 2013 EAG Chairman, K. P. Krishnan, was to provide each EAG

member-state with a pool of professional assessors.

Accordingly, it was no surprise that the number of persons attending the workshop was significant – about 60. The event brought together representatives of the FATF and three FSRBs: MONEYVAL, MENAFATF and EAG. The training was conducted by FATF Secretariat employees Vincent Schmoll and Tom Neilan, representative of the International Monetary Fund Steve Dave and MONEYVAL expert Michael Stellini. The emphasis was placed not only on the analysis of changes following a mutual evaluation and theoretical explanations, but also on the practical aspects, with extra focus on the evaluation of effectiveness, a topic which previously had not been singled out as a separate area, but instead was considered in the context of other procedures.

All participants were split into five teams, each of which subsequently had to prepare draft evaluation reports based on a mock evaluation mission. Discussion of the risk assessment was based on a real-life risk assessment report of New Zealand.

During the workshop, participants went through all real-life stages: risk assessment, analysis of technical compliance and interviews with the representatives of government agencies and private sector. All of these procedures constitute the basis of the 4th round of FATF mutual evaluations, which began in 2014 with the evaluations of Spain and Norway. The Russian Federation will undergo this procedure approximately in 2016-2017.

The workshop ended with the teaching staff expressing hope that the training would help the attendees prepare for participation in mutual evaluations and thanking the organizers from the Russian Federation represented by the ITMCFM and EAG Secretariat for creating comfortable working conditions. Rick McDonnell, FATF Executive Secretary, expressed his support for the above statement, noting the high level of the workshop organization. «I think both the trainers and participants did a great job preparing for the workshop and contributing to it. With every new event, the quality of our trainings improves, while the materials used in them become ever more accurate and on-topic.»

Workshop participants who have undergone training will now join the teams of appraisers from the FATF and three FSRBs (EAG, MONEYVAL and MENAFATF) and may be invited to participate in the 4th round of evaluations.

Vincent Schmoll, Senior Policy Analyst, FATF Secretariat

FB: *You have participated in the first FATF mutual evaluation of Russia. What do you think, has positively changed in the Russian AML/CFT legislation positively changed since that time?*

V.S.: Since the first mutual evaluation of the Russian Federation, its AML/CFT legislation has continued to change. It was already evident from the results of the second evaluation, which was adopted in June 2008, and even more so afterwards with the effort made to address deficiencies identified at that time. For example, Russian authorities were confronted with the particularly challenging task of establishing appropriate measures for dealing with beneficial ownership. Russia was able to enact legislation last year that remedied the deficiencies in this and a number of other areas. In general therefore, I would say that Russian AML/CFT legislation has evolved in a positive direction during the past ten years.

FB: *You are acting as an instructor for the training. How do you estimate the participants' average knowledge and ability? What is your opinion on the activity and the level of training of participants from the EAG and its Secretariat?*

V.S.: I would say that the knowledge and ability of the trainees from EAG and its Secretariat at the last training is on par with those of other FSRBs. We have all had experience with conducting the evaluations of the last round. We therefore share the same challenges in adapting to a new evaluation system that must look beyond pure technical compliance with the FATF Recommendations so as to estimate the effectiveness of our AML/CFT systems. I believe that the EAG participants in the most recent training were able to learn a lot but also contributed to the discussions by raising important issues derived from their previous experience in conducting evaluations.

Sofiene Marouane, Sr. Officer Technical Assistance & Typologies MENAFATF

The MENAFATF Secretariat would like to seize this opportunity to thank the EAG and the Russian Federation for the kind hospitality and excellent facilities provided which greatly participated in the success of the event. Our sincere thanks also go to the FATF Secretariat, the IMF and the different experts. This training is of most importance as countries are requested to implement the amended recommendations and assessors to evaluate whether the required measures are implemented and effective. In addition, this training provided further clarifications and practical insight of the assessment methodology i.e. assessment of both technical compliance and assessment of effectiveness.

MENAFATF has a very good relationship with the EAG as each FSRB holds an observer status in the other allowing it to attend the Plenary and Working Group meetings. Furthermore, MENAFATF and EAG are currently looking forward to enhance their cooperation through future common events and projects. In fact, a joint EAG / MENAFATF Typologies and Capacity Building Workshop is planned to take place in December 2014 which will be an opportunity to gather typology experts from both regions to share views and exchange experiences with respect to ML/FT trends and methods along with capacity building sessions on important and highly demanded themes. In the pipeline also a possible joint typology project which will focus on common AML/CFT issues.

Mishra, the representative of the Indian delegation

***FB:** How does India prepare for the next round of the FATF mutual evaluations? What work is being done to implement the provisions of the legislation to meet the new standards of FATF?*

India has amended the anti-terrorism legislation, namely, the Unlawful Activities (Prevention) Act and the anti-money laundering legislation, namely, the Prevention of Money Laundering Act in 2013. The amendments to these legislations have brought them into the compliance zone of the revised standards of FATF.

As the FATF standards are represented in numerous legislations, Rules and Regulations, the Government has also formed a committee to examine the concerned laws, Rules and Regulations closely in order to identify if there are any gaps in our legislation based on the FATF Recommendations.

The CFT and AML laws as well as the other laws are being implemented not only to combat money laundering and financing of terrorism but to ensure financial integrity and security of the financial sector in India. We are also in the process of initiating our second National Risk Assessment. Further, regular outreach programmes and interaction with all stakeholders take place at regular basis. We are also examining the various nuances of treating direct and indirect tax crimes as predicate offence for money-laundering.

Rick McDonell, Executive Secretary of the FATF

FB: How do you determine the contribution of the workshop into preparations for a new round of evaluations by the FATF and the FSRBs?

R.M.: A. I believe that the workshop was highly successful in three ways. First, it provided experienced professionals with a detailed and practical understanding of the revised FATF standards. Secondly, it gave participants a "hands-on" learning experience in how to apply the new assessment Methodology. Thirdly, it provided an opportunity to discuss and come to some conclusions about what AML/CFT effectiveness compliance means in practice. As a consequence, the workshop was an essential contribution towards ensuring that the new round of evaluations is carried out expertly and consistently.

FB: What further steps will be taken in terms of assessor training?

R.M.: A. The feedback we have received from participants at the Moscow workshop indicates a high level of satisfaction with the course but there are always lessons to be learned and this course is no exception. There is an old saying that "the more you teach the more you learn". We will be adjusting some of the training materials so that they are more explanatory in certain parts. We will be further elaborating the mock evaluation case example so that participants have more tailored information on effectiveness and more guidance on how to write the mutual evaluation report. And, of course, we will continue to provide training courses to other FSRBs and to the FATF itself.

FB: What joint activities are scheduled with other FSRBs?

R.M.: Apart from ongoing mutual evaluation training courses there are a number of other joint or complementary activities with the FSRBs including country training for countries about to undergo a mutual evaluation and assistance with training of assessors in courses organized by individual FSRBs. In addition there will be a natural continuation of the long-established participation our respective plenary and other meetings, joint typology exercises, Secretariat meetings and the Global Network Coordination Group meetings. In my view, each of these activities and all of them combined are demonstrating an increasing level of cooperation and operational maturity within the global network.

FINANCIAL INTELLIGENCE UNITS OF THE EAG STATES

FINANCIAL INTELLIGENCE UNIT OF THE KYRGYZ REPUBLIC (KYRGYZSTAN FIU)

Malice Mambetzhanov, the Chairman of the State Financial Intelligence Service under the Government of the Kyrgyz Republic

2013 for the State Financial Intelligence Service under the Government of the Kyrgyz Republic was a year of significant and positive steps forward towards further development and improvement of the National Anti-Money Laundering and Counter-Financing of Terrorism System (AML/CFT).

This year marks the eighth anniversary of the establishment of the Kyrgyz financial intelligence unit, an authorized AML/CFT agency. The first years in the life of the Agency was a period of its formation, the time of laying the foundation of the legislative framework, training of staff, establishment of interagency and international relations, building of technological capabilities, creation of a single database, and organization of extensive outreach and training activities for reporting entities. Because Kyrgyzstan had never done anything like this before, the work to build the architecture of the national AML/CFT system was neither quick nor easy.

Meanwhile, the fight by the international community against money laundering had been going on already for several years. With the creation of the first financial intelligence units and AML/CFT systems, transnational organized crime, which by that time had already mastered the most complex and intricate schemes for laundering funds and their subsequent integration into the legal economy, finally found a worthy opponent. With the help of the international banking system and governments of the world's leading powers, countries around the world were setting up international organizations tasked with developing standards and essential measures needed to counteract attempts to abuse the global and domestic financial systems. One obvious example of a criminal misuse of a banking system for money laundering purposes in Kyrgyzstan is connected with the laundering and embezzlement

of foreign credit funds at the AsiaUniversalBank, accomplished through an intricate scheme involving transfers of funds from one account to another, their splitting and subsequent siphoning off overseas.

Today, the State Financial Intelligence Service under the Government of the Kyrgyz Republic is going through a period of active development, when we finally can and should talk about the impact of its activities and, of course, of the effectiveness of inter-agency and international cooperation. Firstly, because without interaction between departments, there can be no national anti-money laundering and terrorist financing agency, given that ministries and departments are an integral part, as well as the links, of one and the same chain. Secondly, the establishment and development of the national AML/CFT system and its authorized agency was possible thanks, in no small part, to the technical and advisory support from international organizations and foreign FIUs.

Speaking of the performance of the SFIS under the GRK, It is necessary to give some figures:

Only in the 9 months of 2013 alone, the SFIS conducted 45 AML/CFT and 37 counter-terrorism and extremism financial investigations, submitted to law enforcement 19 consolidated case files related to illegal capital turnover (illegal enterprise, tax evasion, etc.) involving banking instruments totaling more than **184 million soms**, and forwarded to various ministries and agencies, including commercial banks, about 700 requests, of which 17 to international organizations and foreign FIUs.

A good example of the effectiveness of interagency engagement and international cooperation is an investigation conducted by the SFIS into the activities of a transnational criminal group specializing in the smuggling of drugs from Afghanistan to the CIS member-states.

Close engagement in the area of information sharing between the Kyrgyz Drug Control Agency, which had over a long period been gathering intelligence about the criminal group, and the SFIS, which was to trace its illegal proceeds, resulted in the unraveling of a highly complex scheme of banking transactions and financial tricks resorted to by defendants seeking to conceal the traces of criminal proceeds and carry out their laundering.

Significant intelligence-based contribution to the investigation also came from other ministries and agencies of the Kyrgyz Republic, as well as from the Federal Financial Monitoring Service of Russia. One of the suspects in this case, a coordinator of remittance payments between individuals involved in international drug trafficking, was, as it turned out, already under the microscope of the Russian law enforcement. This case resulted in the first in the history of the Kyrgyz Dug Control Agency prosecution of an individual under Article 183 of the Criminal Code (Money laundering), made possible thanks to the materials provided by the SFIS.

In 2013, the EAG organized its first contest for the best example of cooperation between government agencies of EAG member states in the field of AML/CFT. Participants of the 19th EAG Plenary, where the results of the contest were summed up, expressed their appreciation for the work carried out by the SFIS staff and acknowledged the investigation relevance. The investigation conducted by the SFIS under the Government of the Kyrgyz Republic was recognized as the best in its class.

The State Financial Intelligence Service under the Government of the Kyrgyz Republic today has all legal mechanisms necessary to carry out a comprehensive information sharing engagement with foreign FIUs and international organizations on the issue of repatriation of the assets taken out of the country illegally. The Kyrgyz Republic is a full member of the EAG and an active participant in the plenary meetings of the Financial Action Task Force (FATF). The SFIS is a member of the Egmont Group and a participant of the international «STAR» program. All this enables us to conduct a successful search for siphoned off assets with the help of information exchange.

As a result of such searches, the SFIS, while receiving assistance from the Egmont Group, has been able to track the movement of assets siphoned off overseas using an elaborate criminal scheme. Step by step, by dismantling the building blocks of this scheme, SFIS analysts identified one European bank. Following a request from the SFIS, the financial intelligence unit of that country gathered the necessary information about the identified bank account. Later, the SFIS received a reply to its request sent to the FIU of one offshore jurisdiction, confirming that the beneficiary of the account in question was Mr. X, who had withdrawn the funds from Kyrgyzstan while being the head of a commercial enterprise.

That FIU then used its powers to freeze the funds in the account of the European bank and transferred all the relevant information to the Kyrgyz SFIS. The Kyrgyz competent authorities used the intelligence provided by the SFIS to send a mutual legal assistance request

on the basis of United Nations Convention against Corruption for the seizure of Mr. X's assets in the bank pending Kyrgyz court decision on their confiscation and repatriation. The request was satisfied, while Mr. X's funds in the bank were frozen by the decision of a European court.

As of now, Kyrgyzstan is included in the FATF's so-called «grey» list and is subjected to enhanced monitoring. However, this fact should not be viewed as tragedy of the national AML/CFT system; instead, it should be viewed as an opportunity for the country to further develop its national system for combating financial crimes, improve the national legal framework, integrate into it international legal norms and standards, and further harmonize Kyrgyzstan's legislation.

The work to combat crimes aimed at destruction of the global and domestic financial systems can be most effective when it is based on coordinated actions of all countries and on common legal mechanisms and standards. To achieve this ambitious goal, in 2013 Kyrgyzstan has drafted and enacted several legislative acts aimed at bringing its national legislation into line with FATF international standards and recommendations, with Law No. 83 of May 29, 2013 «On amendments to certain legislative acts of the Kyrgyz Republic», which amended Article 183 (Money laundering) and Article 226-1 (Terrorist financing) of the Kyrgyz Criminal Code, probably being the most notable example.

In the framework of the 19th EAG Plenary in November 2013 Kyrgyzstan won a competition for the best cooperation among state agencies in AML/CFT sphere.

The decision to draft and enact this law was dictated by the need to bring its provisions into compliance with the Vienna and Palermo Conventions and the International Convention for the Suppression of the Financing of Terrorism. Additionally, this law amended the Kyrgyz Law «On combating terrorism». In particular, Article 1 was amended to bring the terms and definitions used in the Law of the Kyrgyz Republic «On combating terrorism» in compliance with the UN anti-terrorism conventions and the FATF Recommendations glossary.

The State Financial Intelligence Service is currently working hard to strengthen anti-corruption measures and eradicate its causes. The provisions of all newly drafted bills are tested for adequacy of their anti-corruption measures. The country is preparing a strategy for the development and improvement of the national AML/CFT system, which will include integrated anti-corruption measures developed in accordance with the basic policy of the state as defined in the Decree of the President of the Kyrgyz Republic Almazbek Atambayev dated November 12, 2013 «On measures to eliminate the causes of the political and systemic corruption in government».

The national AML/CFT system cannot be effective without a professionally trained pool of experts. The system for combating financial crimes places considerable skills and knowledge-related requirements on the employees of law enforcement, supervisory and judicial agencies, as well as banks and non-banking institutions. For this reason, in 2013 Kyrgyzstan initiated the opening of the Training and Methodology Center under the SFIS of GKR, which is designed to provide training to the employees of all organizations and institutions that are in one way or another involved in the work of the national AML/CFT system. Training at the TMC will be provided by experienced SFIS staff and leading specialists of the National Bank of the Kyrgyz Republic. In the future, the center plans to boost its teaching capacity by inviting foreign specialists from other training centers and international organizations. This is the first in the Central Asian region training and methodology center of this profile, and already today it can be used to train specialists from neighboring countries. Such plans do exist, and they are quite realistic.

NEWS BLOCK

Rosfinmonitoring and CEC sign Cooperation agreement

On 26 December 2013, the Federal Financial Monitoring Service and the Central Election Commission of the Russian Federation signed a cooperation agreement. The document was signed by CEC chairman Vladimir E. Churov and Rosfinmonitoring director Yury A. Chikhanchin.

The ceremony was attended by CEC deputy chairman Stanislav V.Vavilov, State Secretary and Rosfinmonitoring Deputy Director Pavel V. Livadny, head of the Control Directorate of the CEC Central Office Mikhail N. Artamoshkin, chairman of the board of directors of the Federal Information Center under the CEC Gennady I. Raikov, head of the Federal Information Center under the CEC Mikhail A. Popov, employees of the CEC Central Office, and members of the staff of the Federal Information Center under the CEC.

«Today we are witnessing a very important event,» said V. Churov. «This agreement paves the way for the joint work on the implementation of the Russian legislation and orders of the President of the Russian Federation with regard to exercising control over nominees' property, particularly in three key areas: foreign real estate, foreign accounts and foreign financial instruments.»

The joint work by the CEC and Rosfinmonitoring is aimed at strengthening the fight against corruption and safeguarding the state and society against the threats posed by dishonest people attempting to break the law.

The CEC chairman stressed that one of the main goals of the interagency cooperation is to prevent defamation of law-abiding politicians. «This work is being carried out not so much for fiscal purposes or in order to expose someone, but for the benefit of the nominees themselves – to protect them against all sorts of inaccuracies and provocations, because there are so many dirty tricks that can used to discredit a politician,» said V. Churov.

Yury Chikhanchin noted that Rosfinmonitoring has all the necessary tools needed not only to identify

violations of the law, but also to protect law-abiding citizens, which is especially relevant in the age of electronic payments and anonymous bank accounts. Rosfinmonitoring director expressed confidence that the signed agreement would contribute to the transparency of the electoral process and safeguard election participants against various illegal activities, including against unscrupulous political strategists. «Together we are doing a very important job that benefits the development of democratic processes in the Russian Federation,» said Yury Chikhanchin.

The purpose of the Agreement is to create a framework for cooperation between the CEC and Rosfinmonitoring needed to perform the tasks and functions conferred on the parties by the legislation of the Russian Federation.

According to the document, the parties shall act within the limits of their competences to establish cooperation through the CEC, the Central Office of Rosfinmonitoring, interregional administrations of Rosfinmonitoring in federal districts, and election commissions of the constituent entities of the Russian Federation.

The Agreement provides for the sharing of information on persons nominated for federal government posts, their spouses and minor children; nominees for the post of the highest ranked official of the constituent entity of the Russian Federation, their spouses and minor children; legal entities and individuals that transfer donations to electoral funds, referendum funds, as well the funds of political parties, regional and other registered offices.

EAG Secretariat Meeting Dedicated to the FATF/EAG/MONEYVAl Assesor Training

On February 26, the EAG hosted a videoconference with the participation of the ITMCFM, the Secretariat of the Eurasian Group, Belarus, Kazakhstan and Uzbekistan. The EAG Executive Secretary, B.V. Toropov, familiarized participants with the concept of the FATF assesor training, scheduled for March 2014, as well as the organizational aspects and visa support measures related to the event.

Participants were also informed of the potential of the updated EAG website, including its activity sign-up section, and heard explanations and answers to questions asked by some countries, including about the technical aspects of the new version of the EAG website.

In conclusion, the ITMCFM representative drew participants' attention to the e-learning course titled «Methodology for assessing compliance with the FATF Recommendations and the effectiveness of the AML/CFT systems», available through the EAG official website.

This self-study Russian-language course is designed for the Secretariat staff of FATF-style regional groups, as well as employees of organizations (both public and private) specializing in assessing compliance of national anti-money laundering systems with the FATF Recommendations.

The course, developed under a license agreement with the FATF, is a logical continuation of the ITMCFM's efforts to promote the FATF international standards in the CIS/EAG. In 2012, the ITMCFM translated into Russian the revised version of the FATF Recommendations, as well as developed an e-learning course dedicated to the revised FATF 40 Recommendations, featuring a close integration with the previous tutorial as well as an option for switching between the Russian and English versions (for quick access to the original English text).

All courses developed by the Center can be accessed online from the official EAG website at: http://www.eurasiangroup.org/ru/.

***

On 19 and 26 February 2014, the EAG hosted videoconferencing sessions with the participation of the ITMCFM, the Institute of Financial and Economic Security (IFES) «MEPhI», and financial intelligence

units of Belarus, Kazakhstan and Tajikistan dedicated to the discussion of the training courses expected to be made available via videoconferencing to the concerned FIUs of the Eurasian Group by the IFES.

The IFES has prepared a questionnaire designed to identify the needs of the FIUs in methodical assistance, including the range, scope and sequence of the training courses. It is assumed that the IFES and the ITMCFM will be assisting national FIUs on a wide range of issues. After summarizing the survey results, the training courses will be integrated via videoconferencing in the action plan through the EAG.

New Payment Methods. National Payment System

On February 27-28, the ITMCFM hosted via videoconference a seminar for financial intelligence units, private sector experts and concerned government bodies of Belarus, Kazakhstan, Tajikistan and Uzbekistan titled «New Payment Methods. National Payment System.» The purpose of the seminar was to provide methodological assistance and to build capacity of anti-money laundering systems of Eurasian countries

The role of the main speaker at the seminar was played by Valery A. Lopatin, the deputy head of the International Settlements Department of the Settlement Service Directorate of the state corporation «Bank for Development and Foreign Economic Affairs (Vnesheconombank).»

One of the objectives of the seminar was to familiarize participants with the contemporary model of Russia's national payment system, which is particularly relevant in light of the last year's legislative initiatives. In addition, considerable attention was devoted to alternative currencies, i.e. the so-called «crypto-currencies.»

Participants also discussed issues concerning the integration of databases of various public bodies and financial institutions into a single information environment and remote provision of public and financial services, including through the use of the Universal Electronic Card.

Participants' interest was aroused by the topic dedicated to the differences in the status of bank payment agents and payment processors, as well as the aspects of statutory regulation of the activities of Russia's national payment system participants.

In the course of the seminar, participants were able to ask questions related to both theory and practice, as well as familiarize themselves with the practical side of the work carried out by Russia's national payment system entities.

Advanced training of Rosfinmonitoring's employees

During the period from January 21 till February 11, 2014, in the Rosfinmonitoring conference hall, advanced training was held for employees of the Central Office and inter-regional offices of Rosfinmonitoring (in video conference format) under the program of Combating Money Laundering and Financing of Terrorism. The event was held for employees of Rosfinmonitoring with experience of work of at least 1 year.

At event opening, training participants were welcomed by Deputy Director of Rosfinmonitoring Vladimir I. Glotov.

The International Training and Methodology Center for Financial Monitoring arranged and developed the training program for continuing professional education.

The main targets were development with trainees of a complex of basic knowledge:

- on main lines of Rosfinmonitoring activities and inter-agency cooperation in the sphere combating money laundering and financing of terrorism;
- on procedure and conditions of state civil service and on responsibility of state civil servants for corruption;
- basics of business etiquette and protocol;
- on the national and international system for combating money laundering and the financing of terrorism (fundamentals of organization and holding of financial investigations, fundamentals of macroanalysis and typology studies);
- on supervisory activity in the sphere of combating money laundering and financing of terrorism;
- on responsibility for legal violations in the sphere of combating money laundering and financing of terrorism as well as current issues of information security and protection.

The training was attended by leading experts of Rosfinmonitoring as well as instructors of the Moscow City Management University of the Government of Moscow and the Russian Academy of National Economy and State Service attached to the President of the Russian Federation.

Based on training results, over 100 employees of Rosfinmonitoring obtained advanced training certificates for 74 academic hours.

Basic Principles for Private Sector in AML/CFT sphere

On February 17-18 this year, for the purposes of introduction of financial intelligence units of Belarus, Kazakhstan, Tajikistan and Uzbekistan to the experience of the private sector in implementation of FATF standards, a workshop called I**nternational AML/CFT Standards: Basic Principles for Private Sector** was held at ITMCFM (International Training and Methodology Center for Financial Monitoring).

Invited as the instructor was Viktor L. Dostov – member of the Advisory Committee attached to the inter-agency commission of Rosfinmonitoring, Chairman of the Council of Association Electronic Currency and permanent member of consultations with the private sector of the FATF. During the workshop, the EAG member-states got acquainted both with the experience in implementation of the FATF standards as applied to traditional financial products and with new high-technology challenges for AML/CFT conditions – cyber currencies, cryptocurrencies, quasi-payment instruments.

The event was attended by the FATF President V.P. Nechaev.

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