FINANCIAL SECURITY

NO. 20 APRIL 2018

A. AKSAKOV:

"The State Duma's Financial Markets Committee indents to continue improving the AML/CFT legislation and promptly considering the submitted initiatives, aimed at optimization of the financial monitoring system".

CONTENTS

EDITORIAL BOARD

Члены редакционного совета

DEAR READERS,

Less than a year is left before the start of the newest assessment of the Russian AML/CFT system by the Financial Action Task Force (FATF). Following its findings the conclusion about the extent of our country's compliance with international anti-money laundering and countering the financing of terrorism (AML/CFT) standards will be made.

During the last evaluation of Russia, in 2008, assessors identified a number of shortcomings (including the lack of transparency with regard to beneficial ownership and control over legal persons). After their elimination the FATF Plenary approved our follow-up report in 2013. And in 2014, Russia consolidated its success at the Council of Europe's field-specific platform - MONEYVAL.

Despite this success, we continue our work to improve the Russian AML/CFT regime. It is important to remember that the last round was all about technical compliance (whether the country had adopted the relevant laws, built cooperation with various law enforcement and supervisory bodies, etc.). This time we must demonstrate to the international community the effectiveness of these mechanisms.

To address this task, we must further strengthen our cooperation: from financial institutions, which are a source of information on suspicious transactions, to courts that issue verdicts based on the findings of investigations into illegal financial activities.

I would like to believe that the private sector, along with the government agencies, fully understands today our common responsibility for increasing the transparency of the national financial system.

Yours sincerely,
Yury Chikhanchin,
Director of Rosfinmonitoring,
EAG Chairman 2015-2017

COVER STORY

RESPONSES TO NEW CHALLENGES FACING THE NATIONAL AML/CFT SYSTEM

The Head of the State Duma's Financial Markets Committee on the prospects of improvement of Russian AML/CFT legislation

Anatoly Aksakov

The national anti-money laundering and countering the financing of terrorism (AML/CFT) system, functioning for almost 20 years, faces new challenges today.

On the one hand, the increased terrorist threat, the unfavourable international situation and the emergence of new money laundering channels necessitate the strengthening of oversight by all government agencies over cash flows both within the country and outbound streams.

On the other hand, the rapid digitalization and the virtualization of financial markets and the markets for goods and services call for an adequate review of the ML/TF/PWMD risk assessment and management systems both at the state level and by financial market participants.

At the same time, one of the primary objectives of any legislative work is to ensure the stability of the regulatory environment and to reduce the business costs, based on the estimation of financial consequences for the subjects of regulated legal relationships, with no negative impact on the interests safeguarded by law.

Under Federal Law No. 115-FZ of August 7, 2001 "On Combating Money Laundering and Terrorist Financing" (Law No. 115-FZ), entities carrying out transactions with cash or other property covered by this law are required to monitor transactions potentially linked to risks of illegal activities. This obligation is implemented in two key ways – within the compulsive control and by independent identification of high-risk transactions through the internal controls system. In particular, a heavy burden, in this case, is put on financial institutions as the key participants in the country's financial system. As well as any form of activity subject to standard reporting, the Law No. 115-FZ requirements for mandatory AML/CFT controls, meanwhile, compel banks and other financial institutions to continuously dedicate additional resources to compliance with these requirements. It is too early to talk about denying such actions as a step we are going to make tomorrow.

However, the most part of FATF member countries completely lack mandatory control procedures, focusing instead on the identification of suspicious transactions and prevention.

In such jurisdictions, responsibility for timely detection of clients' illegal activities, including the risks of being prosecuted by the supervisors for improper or untimely response to it, falls entirely on credit institutions. In our situation, along with certain regulatory issues of mandatory control, it is impossible not to recognize that, by defining the operations subject to mandatory control, the state has created a certain "comfort zone" for banks, identifying the most problematic areas within the national risk assessment, where it is necessary to focus attention. Another question is how quickly the list of mandatory controls is updated. The answer should be given jointly by legislators and regulators.

A serious challenge is posed by the ever greater migration of individuals and legal entities into a virtual space requiring both the formation of a state-recognized digital identity and a significant expansion of the range of efficient, safe and user-friendly identification methods.

Under these conditions, the main challenge is the anonymity of users of new virtual payment systems and virtual currencies – "units of value". Now it would be premature to call them means of payment, but they are accepted in the market by single subjects of the economic relations and are of special interest to criminals and terrorists. The systems themselves, working on the basis of these technologies, may not always be qualified as standard financial organizations, and therefore are not regulated by anti-washing legislation.

Here, we need to follow the way common for regulators – that is, to legislate the formats of customer identification, to enter into the anti-money laundering circuit of the organization, on the basis of which digital entities are converted into real values. And this is not a utopia – it is enough to recall that thirty years ago, anonymity was one of the widespread principles of the banking system.

There is no rational reason why means of payment should remain anonymous to financial institutions and government regulators. Naturally, this will ensure the protection of personal and financial confidential information at the appropriate level.

There are responses to new challenges facing the national AML/CFT system. In this regard, I would like to highlight the main areas for AML/CFT legal framework improvements aimed, among others, at eliminating excessive regulatory burden and boosting liquidity of financial institutions, both already under consideration by the State Duma and the ones to be drafted.

IDENTIFICATION

Law No. 115-FZ threshold transaction amount requiring no identification has remained unchanged since 2009. I should note that these are low-risk mass single transactions via which customers individuals purchase goods, pay for services. During this period profound changes have occurred not only in the effectiveness of the national AML/CFT system but also in the prices of all goods and services. In order to improve the effectiveness of the application of a risk-based approach and with account for inflation, it is necessary to consider monetary terms of this criterion and on the basis of real value of standard market transaction to pay for this or that type of services. It seems that today we should talk about various thresholds for different payments. Though, on the other hand, particularly micro-payments are often aimed at terrorist financing.

These changes will not affect the quality of the AML/CFT framework since financial institutions are required to pay attention to all unusual customer transactions, regardless of the amount, with a view to their further analysis for possible links to ML/TF.

It has long been necessary to expand the list of options for performing simplified identification. Given the fact that the uniform federal identification system, despite its rapid development, is still in the stage of formation, it is proposed for the transition period to establish a legal requirement to offer customers who are natural persons the opportunity to use one of the simplified identification methods provided by Law No. 115-FZ, instead of all three.

In addition, the international experience shows that organizations can apply more diverse simplified identification procedures than those allowed under the existing law.

A list of allowed simplified identification procedures that could include the verification of a person's identity by the payment system operator or the operator of the national payment card system is currently underway. Such verification is expected to be carried out on the basis of the information contained in the database of the payment system or the national payment card system, as well as submitted to the financial institution by the customer who is a natural person, including electronically: surname, name, patronymic and, if possible, the series and number of the identity document. At the moment, such opportunity is provided only for holders of Russian internal passports.

Improvements need to be made to the list of required identification information. In particular, we need to reduce the volume of information transmitted to Rosfinmonitoring electronically, by providing the latter with direct access to the databases of the relevant operators of such databases to obtain the information on individuals and legal entities contained in them.

At the same time, it seems reasonable to expand the list of customer identification information obtained by entities carrying out transactions with funds from state authorities through the Unified Interagency Electronic Communication System (UIECS).

The possibility of allowing organizations that are members of banking groups and holdings to use collected identification data has been conceptually

addressed, with the relevant bill drafted on the basis of the provisions of FATF Recommendations 17 and 18 going through a second reading at the State Duma. In addition, entities carrying out transactions with funds and other property should be relieved of the non-core function of supervision over compliance with the migration law. To this end, it is proposed to exclude the migration card data from the list of information required from new customers who are natural persons. At the same time, the information required by Rosfinmonitoring for migration control purposes will be provided to it by the relevant government agency (Interior Ministry) via UIECS. Such project was introduced to the Government by the regulator.

TRANSACTIONS SUBJECT TO MANDATORY CONTROL

The threshold amounts for transactions subject to mandatory controls have remained unchanged since 2001. With account for the inflation indexation various options of changing threshold limits are under consideration. It is a sensitive issue regarding the outcomes of the risk assessment and law-enforcement practice in criminal cases but it is not a prohibited one. The regulators here are open for a dialogue with financial institutions. The ideal platform for such dialogue would be the State Duma.

In the future, it is advisable to discuss in details possibility to abolish controls for the most part of transactions subject to mandatory supervision, and preserve it only for the areas of with high risks of money laundering, corruption, terrorist financing, with reports on transactions suspected of ML/TF

submitted to Rosfinmonitoring. For sure, in this case, mechanisms such as the comprehensive analysis of suspicious financial activity of the client based on the application of indicators, the behavioral profiles of a terrorist, corrupt official, drug dealer, etc., identification of his business ties, which are at the same time criminal, etc. should be legally enforced. This will entail additional costs for financial institutions to develop compliance services. Legislators need to take this fact into consideration.

First of all, we need to discuss the exclusion of compulsory oversight of transactions with real estate for entities carrying out transactions with funds. Rosfinmonitoring can obtain this information directly from the Unified Public Register of Real Estate Titles and Related Transactions (UPRT), since all transactions involving the transfer of ownership are subject to registration.

DESIGNATED PUBLIC OFFICIALS

In 2017, the National Financial Market Council (NFMC) conducted a survey among financial institutions on the subject of legal protection of designated AML/CFT officers.

The survey findings highlighted the relevance of measures aimed at reducing administrative fines for designated officials who committed "technical" violations not directly related to money laundering and terrorist financing.

The extent of the designated officials' liability for violations (including "technical") committed by financial institutions ignores the actual size of salaries paid to such officials in the regions as well as the constantly present risk of dismissal for violations (including "technical"), which leads to a gradual, but constant, decrease in the professional level of responsible officials due to increasing turnover and the declining popularity of their profession.

At present, the issue of assessing the proportionality of administrative penalties provided for designated officials by Article 15.27 of the Code of Administrative Offenses of the Russian Federation is being considered.

In addition, the NFMC's survey has exposed inconsistencies in the systemic implementation of the fundamental principle of independence of designated AML/CFT officials. There are cases where decisions of designated officials are influenced by the management of financial institutions, employees of business units, supervisors and other third parties, including financial institution owners and clients. The responsibility for taking decisions affecting customers (termination of the contract of bank account (deposit)) and refusal to carry out a transaction, as well as for engaging with customers with a view to implementing such decisions, are all too often assigned to the same designated officials.

***

I believe the proposed legislative changes will help, on the one hand, to improve the quality and effectiveness of financial supervision, and on the other, to reduce the costs of its implementation for financial institutions.

In light of the above considerations, the State Duma's Financial Markets Committee, which I am the Head of, indents to continue improving the AML/CFT legislation and promptly considering the submitted initiatives, including those coming from financial market participants, aimed at optimization of the financial monitoring system.

DIALOGUE WITH THE PRIVATE SECTOR AS THE BASIS OF THE RUSSIAN AML/CFT SYSTEM

An interview with Galina Bobrysheva, Deputy Director of the Federal Financial Monitoring Service, and Pavel Livadnyy, State Secretary – Deputy Director of the Federal Financial Monitoring Service

Galina Bobrysheva

Pavel Livadnyy

FS: *Mrs. Bobrysheva, how do you assess the extent of the private sector's involvement in the Russian AML/CFT system? What steps are being taken in this area by Rosfinmonitoring and other supervisory bodies? How effective is the work carried out by compliance units?*

Galina Bobrysheva: The Russian AML/CFT system is modelled on a framework built around the FATF Standards, and, from this perspective, it is structurally similar to comparable systems in other countries. At its heart lie organizations that provide financial services or deal with highly liquid assets – such as precious metals and precious stones and their products, real estate, etc. – with

the overall cumulative effect, as you pointed out, being heavily dependent on the level of their involvement and qualitative input. This is because both financial and non-financial intermediaries must, first and foremost, know how transparent a given transaction is and to what extent a client or a beneficiary is exposed to the risk of involvement in illicit transactions or activities.

If we look back at the 17-year history of the Russian AML/CFT system, there has been a qualitative leap in the level of organizations' involvement. Today, system comprises more than 100,000 financial institutions and representatives of non-financial professions, most of which have established viable compliance and customer due diligence procedures and information sharing arrangements with Rosfinmonitoring, whose communication channels are used to send thousands of suspicious transaction reports daily.

The key objective pursued by Rosfinmonitoring and other Russian supervisors – including the Bank of Russia, Roskomnadzor, Assay Chamber, Federal Tax Service, etc. – is to adopt new preventive measures designed to mitigate ML/TF risks, stop shadow economy participants from implementing their intentions and block dirty money from entering the legitimate financial system. To this end, organizations can utilize their mechanisms for a comprehensive study of clients and the nature of their activities, identify the sources of funds, monitor transactions and, in the case of high risk, refuse to carry out transactions for clients. And, of course, every time a client's transaction or behaviour raises suspicion, they report it to Rosfinmonitoring, as provided by the AML/CFT law.

By adopting a consistent and systemic approach to customer engagement, financial institutions send a message to shadow businesses that transparency of their actions is a guarantee of their business stability and the absence of uncomfortable questions from both the bank and supervisory/law enforcement authorities.

I believe the AML/CFT system has now reached a very important stage of its development. The focus is on preventive measures and the private sector, which, being aware of its role, is finally ready to embark on a mission of enlightenment. I know that banks organize special trainings for students, informing the youth – whose ranks may include future entrepreneurs, lawyers, financiers or simply consumers of financial services – about the dangers of involvement in illicit schemes. I am sure you will agree that this is a completely different level of responsibility, which is projected on future generations.

FS: *Mr. Livadnyy, Russia is getting ready for the upcoming FATF evaluation. In this context, will the assessors' attention be drawn to the private sector engagement?*

Pavel Livadnyy: Yes, that is how it has actually been since the establishment of the FATF. The private sector acts both as an advance detachment standing in the way of dirty money and as part of the structure preventing the execution of illegal transactions through the application of the transaction denial mechanism.

Given that our current efforts are focused on preparing for the fourth round of mutual evaluations, we must acknowledge the private sector's major role in ensuring compliance of our anti-money laundering and countering the financing of terrorism (AML/CFT) system with the FATF Recommendations, at least with 3 immediate outcomes[1], or in fact with all 11.

FS: *How effective is the private sector at blocking illicit funds from entering the financial system?*

Pavel Livadnyy: It is both efficient and effective. However, it is important to remember that this efficiency and effectiveness is only possible in the event of strict compliance with all AML/CFT rules and regulations.

[1] The immediate outcomes concerning the supervision, monitoring and regulation of the private sector by supervisors, the implementation by the private sector of preventive measures to combat ML/TF and report suspicious transactions, the protection of legal entities against misuse for ML/TF purposes, and the unhindered access by competent authorities to beneficial ownership data.

Today, Russia's current AML/CFT legal framework is both highly advanced and well aligned with international standards. However, the AML/CFT system continues to evolve based on the findings of the national risk assessment and the outcomes of cooperation between government agencies and the private sector, including through the Advisory Board of the Interagency Committee for Combating Money Laundering, the Financing of Terrorism and Proliferation of Weapons of Mass Destruction[2], whose effectiveness has been confirmed.

FS: *What kind of knowledge and experience do the employees of banks and other organizations need to have to successfully identify dishonest customers and prevent dubious transactions? Do government organizations share any of their special techniques with other entities?*

Galina Bobrysheva: Compliance units should employ personnel with extensive experience and good management skills, as they have to make some difficult decisions on which the business of their client may even depend. Therefore, they need to have impressive legal and financial skills, as well as a deep understanding of business processes, both within their own and their clients' organizations. But the main thing is that their compliance service must be client-oriented. There should be no room for a formal approach; instead, they need to adequately assess the risks and seek additional sources of information. In essence, compliance units carry out initial financial monitoring and, upon detection of higher risks, take steps to mitigate them. Compliance officers need to have a good understanding of risks and vulnerabilities, and how they can manifest themselves in a given organization. For example, one of the most common money laundering schemes involves the use of pass-through companies, entities that have been specifically created for use in one or two transactions for the purpose of creating a distance between the source of dirty money and the place of its legalization, with laundered proceeds subsequently being either channelled into the legal system or taken overseas.

However, in the situation of tightening controls by banks, tax authorities, Rosfinmonitoring and other supervisors, there has been a rise in pass-through reverse money laundering transactions carried out by legitimate businesses that pay taxes, have office premises and personnel. Their involvement in illicit schemes is typically explained by aggressive tax optimization or simply the desire to avoid paying taxes. One needs to be highly experienced to be able to identify and prevent high-risk behaviour in a flow of perfectly legal transactions. As you can imagine, Rosfinmonitoring, the Bank of Russia, tax authorities, Roskomnadzor and other supervisors assess the respective risks and inform businesses about the emerging trends and illicit schemes. To this end, we regularly update the indicators of suspicious transactions that get reported to Rosfinmonitoring. The International Training and Methodology Centre for Financial Monitoring, established by the Russian Government back in 2005, plays a major role in sharing the knowledge and new typologies. Another important institution with expanding scope is the international network AML/CFT Institute, whose main task is to train personnel for the AML/CFT systems of Russia and its partners in Eurasia.

It is clear that the future belongs to digital compliance systems capable of leveraging their machine learning abilities to adjust to the rapidly changing behaviour patterns of various offenders, whether they are drug dealers relying on electronic payment methods to pay for drugs, dishonest taxpayers or financial scammers. All this requires new knowledge and skills that lie at the intersection of economic, legal, information technology and mathematical disciplines.

FS: *Mr. Livadnyy, which evolutionary direction is the regulatory framework for AML/CFT cooperation with the private sector taking?*

Pavel Livadnyy: On the one hand, we should recall the conclusions, made on the basis of the assessment of law enforcement practice, about the development of financial institutions' compliance units and the success of their efforts to identify ML/TF risks, which served as grounds for a certain liberalization of AML/CFT legislation as it pertains to customer identification requirements. Such liberalization may affect only those segments of the economy and areas of financial institutions' activities that are known for the absence of ML/TF vulnerabilities. Financial institutions' efforts to mitigate ML/TF risks

[2] The Interagency Committee chaired by Rosfinmonitoring Director Yury Chikhanchin.

and, consequently, prevent ML/TF at the heart of the government and its agencies' understanding of the fact that the private sector is ready to operate under less stringent legislative requirements.

FS: *Have the efforts to liberalize the identification procedures already materialized into legislative initiatives?*

Pavel Livadnyy: Most recently, Federal Law No. 482-FZ of December 31, 2017 "On Amendment to Certain Legislative Acts of the Russian Federation" has enabled remote identification of customers with the help of biometric technology, including systems that allow a certain degree of synchronization of data with official sources of information on individual customers. This approach is fully compliant with international AML/CFT requirements and already used in a number of Western European and BRICS countries.

As per FATF Recommendation 10, the absence of face-to-face communication between the financial institution and the client carries a higher risk, which can be offset by the existence of certain conditions such as, in this case, a limited number of financial institutions that meet the established requirements, a limit on the transaction amount and the number of accounts, the use of biometrics to verify the identity of the client, and the absence of the client from a list of designated persons.

Notably, the said regulation is only the first step towards achieving the declared goals and implementation of the idea. Russia is currently working on the development of an integrated biometric system that can be adjusted in line with law enforcement monitoring findings generated in the process of its operation.

We believe that the private sector, insofar as it relates to entities involved in the remote biometric identification process, is capable of ensuring the functioning of the AML/CFT system under the new conditions, which in turn means high confidence in financial institutions.

FS: *But in the sectors where ML/TF risks are high, shouldn't legislative improvements move in a slightly different direction?*

Pavel Livadnyy: In this case, one could really talk about stricter requirements, including those applicable to reporting entities. For example, it is scheduled to remove from the Russian law provisions allowing the use of the currently existing anonymous electronic payment instruments, including web-based, that are not fully in line with international AML/CFT standards.

Further impetus is being given to the efforts to establish a legal mechanism for combating the proliferation of weapons of mass destruction. On April 12, 2018, the State Duma of the Federal Assembly of the Russian Federation passed the Federal Law "On Amendments to Certain Legislative Acts of the Russian Federation Concerning the Fight against the Proliferation of Weapons of Mass Destruction", which provides, among others, for the freezing (blocking) of funds or other property of persons included on the list of organizations and individuals known for their involvement in the proliferation of weapons of mass destruction. The new law requires entities carrying out transactions with funds or other property to suspend transactions if at least one of the parties is a legal entity directly or indirectly owned or controlled by an organization or individual included on the said list, or by a natural or legal person acting on behalf of or at the direction of such organization or person.

The above approaches to improving the Russian AML/CFT legal framework are, in our opinion, indicative of a well-thought-out process that is based on a conscious awareness by the lawmakers of the identified risks, which ensures their mitigation and effective risk management.

FS: *Mrs. Bobrysheva, you talked about the system for AML/CFT personnel training, but how does the government build its engagement with the private sector in other areas? Which modes of such engagement are currently most in demand and hold the greatest potential?*

Galina Bobrysheva: We live in a world of rapid digital progress. Financial intermediation services and the financial sector in general tend to be at the forefront of these trends, literally absorbing new technological solutions and cutting-edge approaches. Under these conditions, the government's job is not just to keep pace with and adapt to the emerging trends but, where possible, to be actively involved in their setting. Rosfinmonitoring, for example, was among the first to use big data processing technologies.

And now, digital technologies allow us to interact with reporting entities practically in real time. For this, we use such a universal and multi-purpose mechanism for communication with the private sector as a "personal account" on Rosfinmonitoring website. It serves simultaneously as an online portal for reporting suspicious transactions, a feedback channel and an element of a digital oversight system.

We use these personal accounts not only to provide guidance and updates on the latest risks, but also to undertake remedial and preventive action. And, I must say, the effectiveness of this mechanism has so far been impressive. With minimal administrative costs, it allows us to focus financial institutions on the elimination of shortcomings identified during internal controls. Only last year, such contactless communication helped achieve compliance for more than a thousand entities. We are constantly working to expand the functionality and convenience of this interface.

One of our priorities is to offer distance learning opportunities. To this end, we make our video training courses on the relevant topics of reporting entities' involvement in the AML/CFT system available online and encourage such entities to test their knowledge with the help of a testing system.

Another important – but more targeted – engagement format is the Compliance Council, an advisory body that brings together representatives of the largest financial institutions and organizations of the non-financial sector. The Council, ever since its establishment, has always been focused on promoting a robust dialogue with representatives of compliance units.

The idea of creating a permanent forum for discussing the issues of information exchange came when Rosfinmonitoring, jointly with the Bank of Russia and

the Federal Security Service, launched a project on a profile of persons traveling to terrorism-prone area. In 2015, we invited heads of compliance units from a number of financial institutions to join this initiative. It should be noted that the outcomes of this cooperation depend, to a large extent, on the proactive position of its main participants – banks.

Today, besides sharing information on new risks and developing the criteria for identifying suspicious transactions, the Council works to improve the quality of reports submitted to Rosfinmonitoring, a task whose progress can be easily measured. For example, over the past two years, we have managed to reduce by more than 50 percent the number of suspicious transaction reports qualified as reports lacking a strong focus on risks.

The important thing is that now we view our mechanisms for communicating with the private sector as a full-fledged format of private-public partnership, which allows us to tackle a whole host of issues facing the national AML/CFT system.

OUR EFFORTS RESULTED IN A STEADY DECLINE IN THE VOLUME OF DUBIOUS TRANSACTIONS

Financial Security magazine's interview with Russian Central Bank Deputy Chair Dmitry Skobelkin

Dmitry Skobelkin

FS: *Mr. Skobelkin, in February 2018 in one of the interviews you said that the rate of encashment transactions has reached 17%.Other sources also confirm that. How did you manage to do that? And what else do you think has to be done to stop financial institutions' involvement in such illicit transactions?*

Dmitry Skobelkin: The Bank of Russia has been very determined and consistent in its efforts to drive down the volumes of dubious transactions. To this end, we have reformed transaction monitoring and analysis system and developed new data processing mechanisms that allowed to speed up (from 3 months to 10 days) the identification and blocking of dubious transactions, as well as to reduce the response time to their transformation.

We work with banks and non-bank institutions (NBIs), using consultative supervision techniques. We take preventive action against those institutions that did not pay enough attention to the Bank of Russia's recommendations, as well as push out of the financial market the entities that ignored its warnings.

Since 2013, as a measure of last resort, the Bank of Russia has blocked access to the market for a total 370 banks. Many of them were involved in questionable transactions. Suspension measures against individual transactions of hundreds of other banks have been applied.

24 financial institutions lost their license in 2017 for legal violations, including in the field of anti-money laundering and combating the financing of terrorism (AML/CFT). In total licenses of 51 financial institutions have been revoked.

Also in 2017, the Bank of Russia applied sanctions against 248 financial institutions for non-compliance with AML/CFT regulations and Federal Law No. 115-FZ, including:

- fines against 161 financial institutions;
- restrictions on certain transactions against 40 financial institutions;
- suspension of certain transactions against 1 financial institution; and
- warnings to address violations of AML/CFT requirements against 126 financial institutions.

This work will naturally be continued also in the future. Many banks have come back to the legal framework, have started to commensurate the profit derived from dubious transactions and the legal risks involved and the possible reputational damage.

Furthermore, there has been a qualitative improvement in the performance of credit and other financial institutions' internal control units. Due to the methodological and practical support provided by the Bank of Russia, they have learned to differentiate bogus economic activities of businesses from the real ones. While only a year ago it took financial institutions at least several months to identify and block dubious transactions, now it takes no more than two weeks, and no more than 2-3 days for high-risk transactions. Our efforts resulted in important reduction of the shadow services market and inconvenience of tax and other budget payments evasion for mala fide entities.

All this has caused increased prices in the shadow market. Transition transactions in the customers' accounts as well have become more expensive which brings their costs to the tax rates.

For its part, the Bank of Russia continues to engage financial institutions and NBIs in risk mitigation and prevention of dubious transactions, primarily by improving the search engines to identify such transactions maximizing their effectiveness and automatization, expanding the list of available data sources, and unifying and standardizing the methodology and approaches to disclosure of dubious transactions.

FS: *The Central Bank of Russia has worked hard to reform the banking sector. It allowed to get rid of questionable and troublesome institutions and thereby reduce the risk of money laundering. However, despite being significantly constrained, illicit financial flows have not completely disappeared, making their way into other sectors. Hence the question: where has this money gone? Which sectors do you think are potentially at greatest risk?*

Dmitry Skobelkin: The Bank of Russia's work has helped to achieve a steady decline in the volume of dubious transactions in the financial sector.

In recent years the volume of illegal funds withdrawal decreased more than 20 times, from RUR1.7 trillion in 2013 to RUR77 billion in 2017, with the volume of encashment transactions in the banking sector falling 3.8-fold, from RUR1.2 trillion to RUR326 billion. At the same time, the Bank of Russia confronts the overflow of dubious transactions from the accountable financial sector to others.

According to the Bank of Russia, throughout 2017, depending on the peaks of tourist season, the monthly volumes of illicit cash flows in the tourism sector ranged from RUR2.7 to RUR5.5 billion, with the total value of such transactions in 2017 estimated at over RUR47 billion, compared to RUR55 billion in 2016.

The monthly volumes of illicit cash flows in the retail sector, meanwhile, according to the Bank of Russia, averaged in the latter 2017 - early 2018 approx. RUR12-15 billion.

RUR billion

	2013	2014	2015	2016	2017	Rate of decline 2017/2016, fold
Capital flight	1,695	816	501	183	77	2.4
Encashment	1,230	681	600	522	326	1.6

The main difficulty encountered by financial institutions in busting such schemes is that their clients working in this business mix illicit transactions with perfectly licit ones.

FS: *Russia has taken some steps recently to liberalize the business environment and create a favourable business climate. In December 2017, the State Duma passed a law that introduces a delisting mechanism for those customers that, despite playing by the rules, ended up in the black list of Rosfinmonitoring and the Bank of Russia. Does this law work? Do you know any examples of successful delisting?*

Dmitry Skobelkin: Even before amendments to the Federal Law on "Combating Money Laundering and Terrorist Financing" aimed at setting up a "rehabilitation" mechanism for clients whom financial institutions denied service, the Bank of Russia adopted measures designed to optimize the use of such sanctions by financial institutions and reduce the risk of refusal for bona fide clients whose details could end up in the "refusals" database.

In particular, the Bank of Russia issued Rosfinmonitoring-endorsed guidelines No. 29-MR dated November 10, 2017[1], setting out the key principles of this "rehabilitation" mechanism:

- inadmissibility of the use by a financial institution of information about "refusals" as a sole ground for refusing to perform a transaction, enter into a bank account (deposit) agreement or for terminating a bank account (deposit) agreement with the client;
- need to examine the transaction for possible risks of money laundering or terrorist financing prior to taking a decision on refusal;
- need for financial institutions to designate (set up) a unit or an official (officials) responsible for reviewing the relevant customer complaints and taking action;
- need for financial institutions to delete "refusals" information previously sent to Rosfinmonitoring in the event of elimination of the grounds for the earlier decision of refusal, or in the event of removal of the grounds for assigning the client to a group of clients at high risk of money laundering or terrorist financing.

Daily monitoring has revealed that financial institutions actively use the mentioned mechanism. In particular, financial institutions have been reporting on "rehabilitated" clients since last November.

At the same time, judging by the feedback the Bank of Russia has been receiving from customers (potential customers), financial institutions thoroughly study clients and their transactions, taking AML/CFT measures only in case of a real (potential) threat of illegal financial transactions or money laundering.

In a number of cases, financial institution customers fail to provide the requested documents, disclose the purpose or economic sense of their transactions or the structure of their property. In such situations, the financial institution refuses to open an account for a client or perform his transaction. Where, however, the client has provided all requested documents and information, the financial institution will analyse the submitted material and, based on such analysis, decide whether to open an account, carry out a transaction or provide access to online banking services.

[1] Bank of Russia Guidelines No. 29-MR dated November 10, 2017 "On approaches to factoring in by financial institutions of information brought to their attention by the Bank Russia on cases of refusal to perform transactions, enter into a bank account (deposit) agreement or on cases of termination of a bank account (deposit) agreement with a customer, in determining the level of the client risk".

This is the final outcome of the review by the Bank of Russia of many customer complaints. Financial institutions report that through their engagement with the customer "the controversial issue has been solved, a bank account agreement has been signed, the transaction has been carried out, a credit card has been issued, access to online banking services has been granted, etc."

The existing mechanism has helped so far to "rehabilitate" over two and a half thousand clients.

In the first quarter of 2018 the number of individuals refused service by financial institutions declined by 35% compared to the same period in 2017.

At the same time in the first quarter of 2018 compared to the same period in 2017 the number of natural persons included in the refusal database reduced 2 times.

In December 2017, the State Duma passed Federal Law No. 470-FZ "On Amendments to Certain Legislative Acts of the Russian Federation", putting in place a two-tier appeal system for refusal decisions taken by financial institutions in respect of their clients:

- the first tier provides for the hearing of the client's appeal in the financial institution, which shall designate a unit or an official responsible for reviewing the relevant customer complaints and taking action;
- the second tier, if the client is not satisfied with the outcome of his appeal hearing in the financial institution, provides for the hearing of the client's appeal against the financial institution's decision by the Bank of Russia's interagency commission, whose decisions are binding for all financial institutions.

With a view to implementing these amendments, the Bank of Russia has prepared the relevant regulatory framework[2].

FS: *One of the schemes for taking money out of the country detected by law enforcement is the so-called "Moldovan Scheme", whereby a Russian firm transfers funds to a foreign company on the basis of a court decision to recover funds owned under a loan agreement – which is fictitious. What is done to prevent this type of illegal activity? Are you carrying out any outreach activities in the banking sector?*

Dmitry Skobelkin: In late 2013, the Bank of Russia detected and identified as funds withdrawal the so-called "Moldovan Scheme", whereby in line with the decision of the Moldavian courts funds from Russian banks were transferred to the accounts of foreign companies opened with a number of Moldovan banks, primarily Moldindconbank.

According to our estimates, Moldova's courts convictions were used in 2013-2014 to siphon off $21 billion from Russia. By mid-2014, the Bank of Russia had put an end to the use of this scheme. The financial institutions involved in it were relevantly sanctioned mostly by revoking their banking licenses.

FS: *The number of cyberattacks on Russian financial institutions has gone up lately. Stolen funds from the accounts end up overseas. What steps does the Central Bank plan to take to recover the funds stolen from Russian financial institutions and sent abroad?*

Dmitry Skobelkin: Not so long ago, the Bank of Russia uncovered several illicit schemes for stealing funds from financial institutions with the help of accounts opened with banks outside Russia.

[2] Bank of Russia Regulation No. 639-P dated March 30, 2018 "On the procedure, timeframe and volume of information to be communicated to financial institutions and non-bank institutions on cases of refusal to perform a transaction, enter into a a bank account (deposit) agreement and (or) of termination of a bank account (deposit) agreement with the client, on eliminating the grounds for the decision to refuse to perform a transaction, on eliminating the grounds for the decision to refuse to enter into a bank account (deposit) agreement, or on the absence of the grounds for termination of the bank account (deposit) agreement with the client"; Bank of Russia Directive No. 4760-U dated March 30, 2018 "On the requirements pertaining to the application, the composition of the interagency commission, the procedure for and timing of the consideration by the interagency commission of the application and documents and (or) information submitted by the applicant, the procedure for the adoption of a decision based on the outcomes of the review and the procedure for communicating by the interagency commission of its decision to the applicant and the relevant financial institution"; Bank of Russia Directive No. 4758-U dated March 30, 2018, "On amendments to Bank of Russia Regulations No. 375-P of March 2, 2012," On requirements for internal control procedures for financial institutions to combat money laundering and terrorist requirements", and Bank of Russia Regulations No. 4759-U dated March 30, 2018, "On amendments to Bank of Russia Regulations No. 445-P dated December 15, 2014" On requirements for internal control procedures for non-bank financial institutions to combat money laundering and terrorist financing", setting out the requirement for financial institutions to cooperate with the client in implementing the mechanism for reviewing previously adopted decisions to refuse service to such clients.

In response, the Bank of Russia jointly with Rosfinmonitoring is looking at possible ways to stop such fund transfers by utilizing the existing international recovery mechanisms. It makes sense to use for this purpose the communication channels of the Egmont Group, a network of financial intelligence units of different countries working together to combat money laundering.

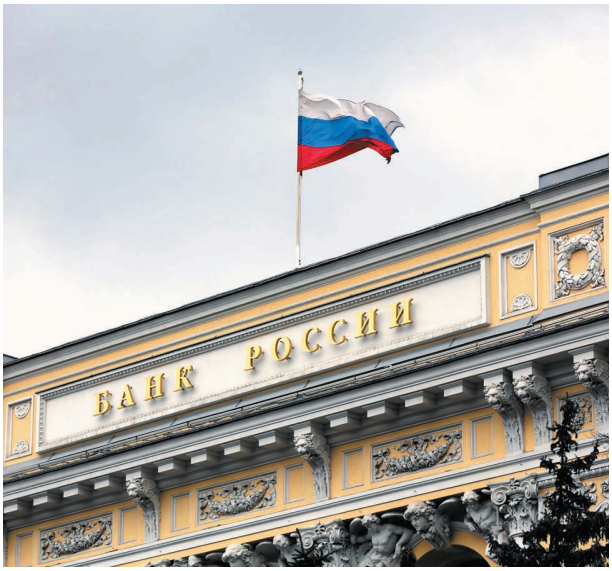
FS: *In 2019, Russia will undergo the FATF evaluation procedures. How would you rate the readiness of Russian financial institutions for it?*

Dmitry Skobelkin: The Bank of Russia is actively involved in preparing the Russian financial sector for the next round of the AML/CFT system evaluations by the Financial Action Task Force on Money Laundering (FATF).

The Bank of Russia is a member of the Interagency Commission to prepare Russia for the FATF evaluations, established by the Russian President. The Bank employees participate in all preparatory activities, and are fully integrated into this process.

Given the important role played by the Bank of Russia, financial and non-bank institutions in implementing AML/CFT requirements, we have a lot of workload in this area.

In 2017, the Bank of Russia established a Working Group, prepared an internal Action Plan and



conducted a self-assessment of technical compliance of the Bank of Russia's legislation and regulations with the FATF Recommendations.

It is worth noting that financial institutions reporting to the Russian Central Bank have a good and detailed understanding of their ML obligations, are aware of their role as a "first line of defence" in the way of "dirty" money, successfully identify external ML/TF threats and risks and take mitigating action.

To this end, the Bank of Russia provides necessary support to the private sector, and this work will undoubtedly be continued.

ASSOCIATION OF RUSSIAN BANKS AND NATIONAL AML/CFT SYSTEM

The Association of Russian Banks is the banking community's centre of analytical and expert work. Members of the Association actively participate in the formulation of coordinated positions on the problems facing the country's banking system at the Association's Council meetings and 12 sector-specific committees

Georgy Luntovsky,
President of the Association of Russian Banks

Georgy Luntovsky

In its work, the Association of Russian Banks pays special attention to the fight against money laundering in the banking sector, participates in the assessment of the regulatory framework for combating illegal financial transactions, takes part in the development of approaches to managing ML risks, and studies international experience in compliance-risk management for the purpose of formulating proposals for its use in the development of the national AML/CFT framework and the risk management system as a whole. Another one of the Association's objectives concerns the discussion and implementation of new approaches and initiatives aimed at reducing the financial burden on credit institutions while maintaining a high level of compliance.

The Russian law is constantly evolving in line with international AML/CFT requirements, including through the adoption of measures designed to increase the effectiveness of interagency cooperation and adopt a risk-based approach in the public and private sectors. In this context, the Association attaches great importance to its ongoing feedback-based engagement with the banking community as a whole and specific financial institutions in particular, as well as to promoting constructive dialogue with market regulators. The urgency of this work increases as in 2018-2019 Russia has to undergo the evaluation by the FATF on-site assessment mission.

First of all, the Association maintains ongoing communication with financial institutions on issues pertaining to their day-to-day activities, as well as assisting in eliciting clarifications from the financial market regulators.

The Association also provides ample opportunities for dialogue with the regulators in the framework of its major events, such as the annual February meeting between representatives of financial institutions and the Bank of Russia management team. This meeting is preceded by extensive preparatory work that involves solicitation of proposals and practical questions from financial institutions, including on combating money laundering and terrorist financing. Rosfinmonitoring and the Bank of Russia view this initiative as a very important one and recognize the practical value of ongoing feedback from the Association member banks, which helps ensure the continuity of a meaningful dialogue with the regulators.

And last but not least, the Association of Russian Banks regularly conducts surveys of financial institutions, thereby promoting a broad discussion by the banking community of the Bank of Russia's legal and regulatory initiatives. Meanwhile, the Association's Compliance Risk and AML/CFT Committee – which serves as an effective forum for discussing the most pressing problems, as well as for studying and evaluating initiatives of the banking and business communities in the field of compliance risk management and drafting proposals for their implementation – attracts input from the expert community.

To carry out an examination of draft laws and regulations and prepare proposals for legislative amendments, the Compliance Risk and AML/CFT Committee utilizes the practical experience and intellectual and professional potential of the Association member banks – among which are large backbone financial institutions operating across Russia, banks backed by foreign capital, as well as small and medium-sized regional banks which promote financial inclusion throughout Russia. The use of such an integrated approach allows the Association to take into account the interests of the entire banking community. In order to provide advisory assistance and solicit feedback, the Compliance Risk and AML/CFT Committee includes a representative of Rosfinmonitoring.

Notably, participation in the preparation for the FATF evaluation is listed among the top subjects in the Compliance Risk and AML/CFT Committee's Action Plan 2018. At its meeting on January 23, 2018, Rosfinmonitoring representatives highlighted the main points of Russia's participation in the national AML/CFT assessment of the banking system, explained the key stages of this process and the specifics of financial institutions' participation in it. The Association of Russian Banks has accumulated proposals for consideration and questions concerning the implementation of Law No. 470-FZ[1], which establishes a "rehabilitation mechanism". These proposals mainly concerned the development of a procedure for implementing Law No. 115-FZ[2] (as amended by Law No. 470-FZ) and clarifying the process of informing customers about the reasons for the financial institution's decision to refuse to comply with the customer's order to carry out a transaction, enter into a contract of bank account (deposit) or terminate the contract of bank account (deposit). Other issues concerned compliance with the List 550-P

[1] Federal Law No. 470-FZ of December 29, 2017 "On Amendments to Certain Legislative Acts of the Russian Federation".

[2] Federal Law No. 115-FZ of August 7, 2001 (as amended on July 29, 2017) "On Combating Money Laundering and Terrorist Financing" (with amendments brought into force on January 28, 2018).

(the list of denied persons)[3]. With a view to avoiding any negative implications for financial institutions in the future and, as a consequence, any changes to the internal control procedures adopted by them, the Compliance Risk and AML/CFT Committee, at its meeting held on January 23, 2018, discussed the issues concerning the practical application by financial institutions of Law No. 115-FZ (as amended by Law No. 470-FZ). All proposals and questions were forwarded to the Bank of Russia for their consideration in the drafting by the regulator of a by-law.

By combining the best experience and expertise of the Association members within the framework of the Compliance Risk and AML/CFT Committee to develop new solutions in compliance risk management, while staying true to the Bank of Russia and Rosfinmonitoring guidelines, we shall help address the challenges facing the banking community, including the successful completion by Russia of the AML/CFT evaluation of its banking system.

[3] Regulations on the Procedure for Communicating to Financial Institutions and Non-Bank Institutions of Information about Refusals to Comply with the Customer's Order to Carry Out a Transaction, Enter into a Contract of Bank Account (deposit) and (or) Terminate a Contract of Bank Account (deposit) with the Customer (approved by Bank of Russia Decree No. 550-P dated July 20, 2016).

THE IMPORTANCE OF EFFECTIVE INFORMATION SHARING AND PUBLIC PRIVATE SECTOR PARTNERSHIPS IN THE FIGHT AGAINST TERRORIST FINANCING

The role of the private sector, in particular financial institutions, has always been central to the fight against money laundering and terrorist financing

David Lewis,
Financial Action Task Force (FATF) Executive Secretary

It is therefore vital that the Financial Action Task Force (FATF) continually seeks to improve engagement between the public and private sector.

Financial institutions hold information that is critical to understanding the "financial behaviour" of terrorists and those that fund terrorism. We need to ensure this information is fully and effectively exploited without undermining individuals' data protection and privacy rights.

At the FATF, engagement with the private sector became a top priority immediately following the Paris attacks of 2015. A joint meeting between FATF member governments and representatives of the private sector highlighted the importance of tackling long-standing barriers to effective information exchange within banks that operate in multiple jurisdictions, between banks, and with the authorities in each country, as well as between agencies domestically and internationally.

Reference

The terrorist acts in Paris and its suburbs were committed late in the evening on Friday, November 13, 2015. Almost simultaneously, several attacks were carried out: explosions near the stadium "Stade de France" in Saint-Denis, shootings in several restaurants, as well as the massacre in the concert hall "Le Bataclan" (where about 100 people were taken hostage). 130 people were killed, more than 350 wounded. According to media reports, these were terrorist attacks that claimed the largest number of victims in the history of France and the largest attack on Paris since World War II. The country, for only the fourth time in its history, introduced a state of emergency. The "Islamic State" claimed responsibility for the attacks, calling them "French 9/11".

Following this meeting, the FATF, through its members, shared with financial institutions and others, the results of its research on indicators of terrorist financing risk. This was further supported by the FATF publication of its consolidated standards on information sharing in 2016, which grouped the relevant sections of the FATF Recommendations dedicated to the exchange of information. The compilation will help to clarify what the FATF Recommendations require in terms of the types of information that should be shared, including the types of information that competent authorities are required to make publicly available, the circumstances in which such information should be shared, and the protections and safeguards which should apply to information sharing and exchange.

Since then, the FATF has continued to work in close partnership with the private sector, in particular with the *Institute of International Finance* and the *Wolfsberg Group*, to promote more effective information sharing and to help identify and address the barriers to this. This has since led to the publication of guidance on private sector information sharing in November 2017.

The FATF regularly meets with representatives of those businesses that are at the front line of detecting and disrupting the funding of terrorism, through its Private Sector Consultative Forum (the Forum) and through the Forum of Heads of Financial Intelligence Units, among other events.

The main issues on the agenda of the Forum are as follows:

- Financial inclusion
- Correspondent banking
- De-risking and its numerous drivers
- Beneficial ownership
- Information exchange
- FinTech and RegTech.

Recently, the Forum has focused on strengthening information exchange between groups of financial service providers, private sector participants; private and public sector as well as within the public sector. While progress has been made, much more needs to be done if financial intelligence units and law enforcement agencies are to fully exploit the information held by financial institutions in particular, and make better use of their efforts and ability to identify suspicious transactions.

At these FATF events, private sector representatives stress the importance of a common approach to **cooperation with the public sector and law enforcement agencies**. The exchange of information with financial intelligence units is of particular importance. Encouragingly, there are a growing number of examples of public-private partnerships that facilitate such information exchange and we are seeing real results from this. Such initiatives need to be built on and developed, not only a national level but also across borders.

Collaboration with Non-Profit Organisations (NPOs) is increasingly important in order to address terrorist financing channels. As a result of collaboration with the NPO sector, the FATF has reviewed and enhanced its standards and the sector is now represented in the Forum. It is equally important that credit and financial institutions establish closer working relationships with the NPO sector.

The effective implementation of FATF standards as they apply to remittance providers, lawyers, accountants and company formation agents is also

an important and growing area of focus for FATF, and the subject of discussions with the private sector. It is important to better understand the role of these businesses in money laundering and terrorist financing, wittingly or unwittingly, and to ensure effective supervision and enforcement of these businesses to protect them from such abuse. FATF is actively working to develop a better understanding of professional money laundering networks that are offering money laundering as a service to criminals and terrorists alike, and where organisations such as Europol have identified 400 professional money launderers operating at the top level in Europe alone.

In the era of digital technologies, the FATF is closely monitoring the use of innovative financial products for money laundering and terrorist financing. The FATF recognizes the opportunities such services provide, not least for financial inclusion, while also seeing the risks. As such the FATF has publicly stated its strong support for financial innovation in line with anti-money laundering and counter-terrorist financing measures. FATF has held a number of forums with the FinTech and RegTech community to raise awareness and understanding of these risks and to work together to address these, while supporting financial innovation. To this end, the FATF has also recently launched an online platform for its members to provide up-to-date information on their own initiatives. More detailed information on the project can be found at the organization's website.

The FATF will continue to work in partnership with the private sector and to promote national and international initiatives to improve the exchange of information to more effectively tackle money laundering and terrorist financing. A common sense, risk-based, intelligence-led approach should be at the heart of these efforts. Our collective efforts to tackle these threats should not become a slave to inflexible regulatory compliance and a box-ticking mind-set. This will be at the forefront of FATF work in the coming months, with the support of the G20, as it reviews its guidance on virtual currencies - or crypto assets - and considers if changes to the standards are necessary. The communique of G20 Finance Ministers and Central Bank Governors, that met in Argentina in March, reflected the commitment of the world economic leaders to implement the FATF standards as they apply to crypto assets. The G20 is looking forward to FATF's review of these standards, and called on the FATF to advance their global implementation. The FATF will be updating them later in the year on progress with its work in this area. FATF is now looking forward to President Macron's high-level conference on terrorist financing, that will be held in Paris at the end of April.

Reference

David Lewis joined the FATF as its Executive Secretary in November 2015, following posts for the UK Government as Head of the Illicit Finance Unit and Senior Policy Advisor on money laundering and terrorist financing. He was previously a senior member of the National Crime Agency.

As Executive Secretary, Mr. Lewis is responsible for leading the FATF Secretariat, coordinating and delivering the work of the FATF on money laundering and countering the financing of terrorism and proliferation of weapons of mass destruction.

COMPLIANCE AND PARTNERSHIP WITH THE PRIVATE SECTOR IN FEDERAL DISTRICTS

For the purposes of improving the quality of information flow on behalf of the financial institutions as well as to attract the expert community the Compliance Council was established in 2016. It included the heads of compliance units, CEOs responsible for AML/CFT issues in financial institutions and the most active participants of the anti-money laundering systems. Similar councils are set up in each 9 federal districts on the basis of the Rosfinmonitoring Interregional departments. This initiative allowed to bring attention of the expert community to the AML/CFT issues not only on the federal but on the regional level as well

Central Federal District

Yevgeny Legostaev,
Head of the Interagency Working Group for Combating Illegal Financial Transactions in the Central Federal District

The regional Compliance Council of the Central Federal District is home to nine working groups made up of representatives of: the banking sector, microfinance companies, remittance services providers, e-money operators, mobile network operators, leasing and factoring companies, the jewellery sector, real estate agents, the gambling industry, auditors, notaries and lawyers.

The working group that includes representatives of mobile network operators and the banking sector were particularly effective. The working group with mobile network operators comprises Rostelecom PJSC, MTS, T2 Mobile, Megafon, VimpelCom, MGTS, Tinkoff Mobile and Transtelecom Company.

North-Western Federal District

Igor Loskutov,
Head of the Interagency Working Group on Financial Monitoring for the North-Western Federal District

Despite the fact that the NWFD Compliance Council includes both banking and non-banking financial institutions, due to the tasks assigned by Rosfinmonitoring and its Interregional department, a majority of the meetings organized in 2017 were held with the participation of representatives of the banking sector.

One of the main discussion topics was the efforts to improve the method for identifying dubious transactions carried out by financial institution customers, based on the identification of specific typologies of suspicious activity. The need to improve the methodology in this area and strengthen cooperation between Rosfinmonitoring and the private sector is due to a steady increase in the volume of transactions. It is also important to avoid mistakes in decisions taken by financial institutions to classify a transaction as suspicious or to terminate the relationship with the customer in line with actual AML/CFT requirements.

Volga Federal District

Viktor Tsyganov,
Head of Rosfinmonitoring Interregional department in the Volga Federal District

The VFD Compliance Council brings together representatives of different financial institutions, which, in our view, facilitates a better understanding of AML/CFT risks in the context of the scope of each bank's operations and ensures a better coverage of the sector in general.

The main purpose of the Council is to design measures to discourage businesses from engaging in illegal activities and to timely respond and adapt to the constantly evolving financial market and changes brought about by the digital economy.

Among the Council's priorities is the development of measures aimed at reducing the risk of illegal transit operations.

Ural Federal District

Alexey Kardapoltsev,
Head of the Interagency Working Group on Financial Monitoring for the Ural Federal District

Financial institutions participating in a meeting of the Regional Compliance Council highlighted the frequent use of judgement enforcement mechanisms to circumvent measures aimed at preventing the execution of doubtful transactions that run afoul of the AML/CFT law.

The Interregional Department undertook a review of reports on transactions related to the transfer of funds in response to writs of execution, revealing a range of standard schemes and ways to suppress them. The review findings, along with other information submitted by financial institutions, were communicated to all Compliance Council members for the adoption of internal control measures. Cooperation was also sought from the Ural District Federal Service of Court Bailiffs and Courts, including in coordinating joint action.

Siberian Federal District

Andrey Dolbnya,
Head of Rosfinmonitoring Interregional Department in the Siberian Federal District

Among the regional Compliance Council members are representatives of financial institutions operating in the region – which make up the majority of Council members – supervisors and some non-financial institutions.

The main agenda of the Council's meetings in the past period was aimed at improving compliance by financial institutions with AML/CFT requirements. It included promoting a common understanding of ML/TF risks, targeted cooperation between supervisors and financial institutions in specific illicit financial transaction typologies and schemes, and providing feedback on STRs.

Far Eastern Federal District

Viktor Chevelev,
Head of Rosfinmonitoring Interregional Department in the Far Eastern Federal District

The specifics of the regional Compliance Council at the Rosfinmonitoring FEFD Interregional Department are determined by its composition, which includes representatives of the branches of major financial institutions operating in the Far Eastern Federal District.

One of the Compliance Council's key priorities is to develop and implement new measures to combat money laundering and terrorist financing. Thus, at its meeting "Development of New Criteria for Detecting Suspicious Defence Procurement Transactions", participants discussed banks' role in detecting risks associated with the implementation of defence procurement contracts, resulting in the formulation of proposals for legislative amendments in this area.

North Caucasian Federal District

Andrey Volobuev,
Head of the Interagency Working Group on Financial Monitoring for the North Caucasian Federal District

Rosfinmonitoring's NCFD office uses all available tools to bolster interagency cooperation and strengthen direct contacts with representatives of the private sector in order to improve their compliance with AML/CFT requirements and enhance information sharing between reporting entities and Rosfinmonitoring.

One of the most effective tools for communicating the ML/TF risks to the private sector and eliciting its feedback is the NCFD Compliance Council, established on the initiative of our agency in the autumn of 2016.

Crimea and Sevastopol

Herman Shatsky,
Head of Rosfinmonitoring Interregional Department in Crimea and Sevastopol

Among the main outcomes of the Compliance Council's activities in 2016 were the development of a systematic approach to the formulation of proposals for improving the regulations setting out the procedure for the submission of information to the designated authority, as well as the development and implementation of a system of indicators that allow financial institutions to identify the risks of illegal activity among their customers (the profile of a tax evader, terrorist, corrupt official, etc.).

Particular attention of the Council was devoted to the shifting of the focus of financial institutions' reporting from isolated transactions to their customers' suspicious activity and its preliminary analysis (an independent financial investigation).

OUR RESULTS ALLOW FOR ANALYZING INFORMATION AT MUCH HIGHER LEVEL

Sergei Monin,
Chairman of the Board, Raiffeisenbank

Sergei Monin

Bank Business Profile

AO Raiffeisenbank is a subsidiary of Raiffeisen Bank International AG, Austria, and operates in Russia since 1996. The Bank of Russia included Raiffeisenbank in the list of systemically important credit institutions. Raiffeisenbank obtained the highest national credit rating AAA (ru) (ACRA). In 2017, Raiffeisenbank was among the top 20 leading banks in Russia. Besides that, the Bank of Russia and Forbes ranked Raiffeisenbank among the top 10 most reliable banks in 2017. Raiffeisenbank offers a full range of services to retail and corporate customers, both resident and non-resident, in rubles and foreign currencies. At present, Raiffeisenbank has over 179 branches in 44 Russian regions and serves more than 1.6 million individual customers.

Prerequisites for Modification of Financial Flows Monitoring System

Despite the efforts undertaken by the global community to establish the effective counter-terrorist financing system, some of its fundamental principles no longer adequately address the new challenges and threats emerged in the second decade of the 21st century.

The globalization processes and continuous development of the international financial system triggered substantive changes in the cash flow processes, making it easier to move funds across borders, enabling to carry out transactions much faster, and providing for broader financial inclusion.

The measures aimed at strengthening controls in the banking sector of the economy implemented at the international and national level forced terrorist organizations and networks to modify their funds collection and movement schemes and to invent new methods for evading and overcoming restrictions established under the counter-terrorist financing systems.

In February 2015, the Financial Action Task Force (FATF) stated that "terrorism is an increasingly global problem that requires concerted global action by a united international community. The ISIL phenomenon shows a new type of terrorist organization with unique funding streams that are crucial to its activities; cutting off this financing is therefore critically important".[1]

In such situation, efforts should be focused on identifying, disrupting and preventing reemergence of channels through which terrorist groups receive financial support as well as on improving the national financial system controls and developing new terrorist financing typologies and counter-terrorist financing techniques.

In the Russian Federation, this work is coordinated by Rosfinmonitoring in consultation with the Bank of Russia, which is the financial market regulator, and other government authorities.

In line with the FATF counter-terrorist financing operational plan and based on the indicators developed for identifying and disrupting financial flows of terrorists and terrorist organizations, several largest Russian banks, including Raiffeisenbank, became engaged in implementation of the financial flows monitoring system modification project in 2016.

Launch of the Project

In the first half of 2016, the managers and experts of the compliance department of Raiffeisenbank took part in the meetings arranged by Rosfinmonitoring jointly with the Bank of Russia and law enforcement agencies for the representatives of the banks that were involved in the development and implementation of the pilot project aimed at modifying the financial flows monitoring system.

At those meetings, the project participants discussed ways of identifying illegal schemes based on the developed indicators, behavioral patterns and other features of customers, methods of utilizing the lists of territories with increased terrorist activities as well as special terminology.

These joint efforts resulted in the development of the algorithm intended for identification of potential TF-related transactions based on the two-level indicator system.

Given the proactive attitude of the representatives of Raiffeisenbank compliance department, the Bank was invited to participate in testing of the jointly developed transaction identification mechanisms under the pilot project.

Planning of Implementation of the Pilot Project in Raiffeisenbank

Following the meeting with Rosfinmonitoring, the senior management of Raiffeisenbank immediately met with the staff of the compliance and IT departments and decided to establish an expert team for practical implementation of scenarios provided by Rosfinmonitoring with due consideration for the best practices and the Bank's experience in application of information technologies and AML/CFT internal controls.

[1] The FATF counter-terrorist financing operational plan, the FATF Plenary, February 2015

In order to speed up the software development process and to avoid unnecessary formality, it was proposed to use the Agile methodology, where the required specialists joined the "core" expert team, if necessary.

On the next day after making this decision, the senior management of Raiffeisenbank established the core expert team comprised of the manager of the compliance department and three employees of the IT departments (one analyst and two developers).

To expedite the implementation of the pilot project, the experts decided to divide the development process into segments as per the assigned functions, design the software components in parallel and implement them in a stepwise manner.

Implementation of the Project

The process of designing the IT logic program based on the indicator algorithms involved analysis of the indicators, development of a data model for identifying these indicators and writing the logic program itself. To identify the data sources, over 300 automated systems of the bank were analyzed, of which three systems containing the necessary information were selected.

After that, the algorithms were implemented in the bank's automated systems, and the terms of reference were developed for upgrading those systems that initially had no built-in algorithms.

The joint efforts of the IT and compliance departments yielded the interim result – one month data on customers and their transactions identified based on the transactional and behavioral scenarios. The next two weeks were spent for refining the scenarios and improving quality of data contained in the relevant reports to be submitted to Rosfinmonitoring.

However, the data were received in the format (XML) which made their processing quite difficult with the application of publicly available software (it was impossible to automatically analyze and verify data and rectify incorrect data). Therefore, we selected the supplier of the software solution for validating information.

Since the supplied software solution was not fully compatible with the automated systems used in Raiffeisenbank, we had to develop a special integration adapter that would allow for uploading the received schemes into the systems.

For exchanging information online, the access to the Raiffeisenbank's personal account on the web portal of the Federal Financial Monitoring Service was extended upon approval of Rosfinmonitoring. The Bank installed required software and made necessary settings on the workstation of the Bank reporting officer. The cryptographic protection tools were installed on the workstation of the said officer so that he could use the electronic (digital) signature for signing documents, and the qualification certificate of the officer responsible of AML/CFT internal controls was used for drawing up reports.

In mid-2017, one month following launch of the pilot project, Raiffeisenbank submitted the first electronic report containing data on actual customers and their transactions. The report was drawn up based on information from several automated systems of the Bank and was validated in compliance with the XSD schemes developed and provided by Rosfinmonitoring. Based on the feedback received from Rosfinmonitoring, the Bank took actions for rectifying errors in the electronic report format and improved quality of electronic report by including in it more meaningful information generated by the Bank's automated systems. The improved reports successfully underwent logical tests performed by Rosfinmonitoring which was confirmed by the report acceptance certificates.

Completion of the Pilot Project Development

In the first quarter of 2017, Rosfinmonitoring held several working meetings with the managers and staff of the IT and compliance departments of Raiffeisenbank to find potential solutions of the problems encountered by the Bank in obtaining certain information about customers and their transactions under the developed scenarios and to consider improvements in XSD schemes proposed by Raiffeisenbank. The parties also discussed whether or not the Bank could identify the used indicators taking into account the specificities of its business. Following these meetings, Raiffeisenbank received recommendations for more effective identification of transactions and schemes and better quality of data contained in electronic reports.

Assessment of Effectiveness (Summary)

The project resulted in implementation of scenario analysis mechanism based on over 90% of indicators provided by Rosfinmonitoring. The remaining 10% of indicators can hardly be used (or cannot be used) for automated detection of potential TF-related transactions and schemes based on the information available to Raiffeisenbank.

In our opinion, the yielded results allow us to analyze received information at a new much higher level. The schemes identified with the application the indicators and scenarios have become much clearer and cover behavioral patterns of customers based on the predetermined parameters. Comprehensive scenario analysis makes it possible to reduce the volume on meaningless information and to optimize the work process.

Raiffeisenbank expresses gratitude to Rosfinmonitoring, Bank of Russia and other competent authorities for the invitation to participate in the financial flows monitoring system modification project as well as for the received recommendations and assistance. The gained experience will help Raiffeisenbank to improve its AML/CFT internal control system, and hopefully will be useful not just for the Russian financial institutions and authorities, but also for the international community.

VTB BANK RUNS FINANCIAL INCLUSION EXPERIMENT

Alexander Yakovlev,
Senior Vice-President, Head of Compliance and Financial Monitoring Department of VTB Bank

Alexander Yakovlev

At present, increased attention is paid to implementation of new technologies and financial inclusion both internationally and domestically. In particular, in 2018, the Bank of Russia drafted the Financial Inclusion Strategy for 2018-2020. One of its objectives is to expand access and enhance quality of financial services offered to, *inter alia*, small and medium businesses.

It should be noted that the first steps in this direction were made in October 2016, when the Russian Government adopted Resolution 1104[1] for developing and implementing the automated procedure of remote (online) registration of legal entities and individual entrepreneurs and for reducing time required for opening bank accounts. The special interagency working group comprised of representatives of the Russian Ministry of Communications and Mass Media, Federal Security Service, Federal Tax Service and Rosfinmonitoring was established for pursuing the objectives set forth in the Resolution. Besides that, two commercial banks, namely Sberbank and VTB Bank (hereinafter the Bank), became involved in this experiment.

[1] RF Government Resolution No.1104 dated 29.10.2016 "On running the experiment in 2016-2018 for ensuring submission of electronic documents for government registration of legal entities and individual entrepreneurs and opening accounts with credit institutions with the use of the special secure automated system intended for centralized issuance and storage of advanced qualified electronic signature keys (hereinafter QES) and their remote use by holders of qualified electronic signature validation key certificates"

Identification of potential threats and mitigation of ML/TF risks in compliance with Federal Law No.115-FZ of 07.08.2001[2] has always been the priority for the Bank. Therefore, in the context of this experiment, it was necessary to develop and validate an automated system information security threat model, including a model for prevention of ML/TF risks. In the framework of the experiment, the Bank developed a special interface for registration of legal entities and individual entrepreneurs and subsequent opening bank accounts and implemented this interface on its official website. For this purpose, additional functions were built into the prototype Web system for preparing a package of documents required for registration, paying registration fee, issuing qualified electronic signature after identification and also for submitting documents in the electronic format to the Russian Federal Tax Service and confirming registration by the Federal Tax Service in a remote manner.

As mentioned above, the Bank had to develop a threat model for preventing ML/TF risks (hereinafter the model) intended for exploring potential risks and vulnerabilities in the process of opening bank accounts and carrying out dubious transactions by registered legal entities and individual entrepreneurs as well as for developing measures aimed at prevention, identification and elimination of such risks and vulnerabilities.

Following the preliminary analysis of potential risks, the Bank identified such threats as potential registration of large number of companies created for carrying out dubious transactions. These companies open many accounts as shorter time is needed for registering a company and opening a bank account and operating costs are reduced. Another identified threat is misuse of qualified electronic signatures by beneficial owners. Besides that, increased threat was posed by potential structuring of transaction schemes by reducing volumes of dubious transactions of individual customers and increasing number of parties involved in such schemes, which would make it more difficult to promptly identify such structured transactions.

For pursuing these objectives, the process was divided into separate stages, and the list of control measures aimed mitigating ML/TF risks and threats at each stage was drawn up under this FinTech project.

When receiving documents for registration of legal entities and individual entrepreneurs, the Bank implemented the following controls:

- verification of a potential customer on the lists of designated entities and individuals and additional screening by the Banks's security department;
- one person can register remotely (online) only one legal entity/ individual entrepreneurship;
- denial of registration of legal entities and individual entrepreneurships by members (managers, beneficial owners) whose transactions with funds or other assets are subject to suspension, and who are prohibited from opening bank accounts under Article 7(5) of the Federal Law;
- denial of registration of legal entities and individual entrepreneurships by members, against whom restrictive measures have been previously imposed by the Bank.

At the stage of opening bank accounts, the Bank implemented the following controls:

- full identification of legal entities and individual entrepreneurs, their representatives, beneficial owners and beneficiaries;
- customers are requested to complete online a special questionnaire, where results of analysis of provided responses may require a face-to-face interview and/or onsite visit to legal entity/ individual entrepreneur premises;
- the Bank may refuse to open an account if it suspects that bank account is opened for ML/TF purposes, after which it notifies the designated agency of such refusal in compliance with the applicable legislation;
- number of accounts that can be opened by legal entities or individual entrepreneurs under this experiment is limited;

[2] Federal Law No.115-FZ of 07.08.2001 on Combating Legalization (Laundering) of Proceeds Obtained through Crime and Financing of Terrorism (hereinafter the Federal Law)

- monthly amount of transactions that may be carried out through a current account is limited by the amount indicated by a customer in the AML/CFT questionnaire;

- higher risk rating is assigned to legal entities and individual entrepreneurs that open accounts, and transactions carried out by them through such accounts are subject to enhanced monitoring.

At the stage of providing services to customers, the Bank implemented the following controls:

- if an amount actually deposited into account exceeds the amount declared before opening the account, a manager of legal entity/ individual entrepreneurship is invited to visit the Bank office for repeated verification of his identification data; and if he refuses to do so, the Bank applies measures specified in Article 7 (5.2) and (11) of the Federal Law;

- when the Bank provides Rosfinmonitoring with reports on both transactions that are subject to mandatory monitoring and suspicious transaction carried out by legal entities and individual entrepreneurs for whom bank accounts are opened under the experiment, it fills in the special field of the report template (intended for proving additional information) with the relevant codes.

Upon successful approval of the controls developed under the threat model, the Bank launched the pilot project, as a result of which:

- over 22 thousand users paid interest in the new service;

- about 1,700 legal entities and individual entrepreneurs registered their businesses or opened current accounts with the Bank in a remote manner.

It should be additionally noted that the following factors had the decisive impact on the new service in course of implementation of the pilot project:

- qualified electronic signatures are not widespread among potential customers;

- there are no technologies for issuing, using and storing cloud-based qualified electronic signatures;

- no mechanism for remote identification/ authentication was available during implementation of the pilot project.

In summary, it can be stated that the Bank has successfully achieved the objectives under the pilot project and continues to offer the new service for onboarding small business customers.

LAWYERS' CONTRIBUTION TO THE FIGHT AGAINST MONEY LAUNDERING

The Council of the Nizhny Novgorod Region Chamber of Lawyers recognizes the importance of activities aimed at increasing the level of involvement of the Chamber's lawyers in the AML/CFT system, particularly in the run-up to the FATF fourth round of mutual evaluations

Nikolai Rogachev,

President of the Nizhny Novgorod Region Chamber of Lawyers, Vice-President of the Russian Federal Chamber of Lawyers, and FCL representative for the Volga Federal District

Nikolai Rogachev

Sharing the aspirations of all national AML/CFT system participants – which also includes the community of legal professionals – to tackle new challenges, the Chamber of Lawyers of the Nizhny Novgorod Region, working closely with the relevant state authorities, i.e., Rosfinmonitoring's Volga Federal District Interregional department, is ready to be engaged in these efforts.

The first task that has been promptly and successfully solved by the Chamber of Lawyers upon the request by the Head of Rosfinmonitoring's VFD office, Viktor Tsyganov, was to increase the number of personal accounts opened by lawyers on Rosfinmonitoring's official website.

To this end, the Chamber of Lawyers utilized all available information resources (the magazine and website) to communicate to lawyers the importance

and necessity of complying with the Federal Chamber of Lawyers' recommendation for each lawyer to open a personal account on Rosfinmonitoring's website.

A significant role in addressing this task was played by the heads of legal practices listed in the register of the Chamber of Lawyers of the Nizhny Novgorod Region (and their branches), all of whom were duly informed about this task.

In addition, the Chamber of Lawyers provided technical support in setting up personal accounts for those lawyers who needed it.

At the moment the Chamber of Lawyers, in close cooperation with Rosfinmonitoring's VFD office, is currently following the number of its members with a personal account and the frequency of their visits. The Chamber is taking steps to ensure that each lawyer, after taking an oath, opens a personal account on Rosfinmonitoring's website. The issue of lawyers' compliance with AML/CFT regulations has been classified by the Chamber as urgent. The President of the Chamber has agreed to be included in the VFD Compliance Council.

At the same time, I would also like to highlight the specifics that do not allow Russian legal professionals to compare to their Western counterparts in informing the financial intelligence unit about suspicious and dubious transactions. The scope of Russian lawyers' activity is much narrower than that of their foreign colleagues, who exercise functions typically assigned in Russia to notaries.

Firstly, a majority of Russian lawyers specialize in criminal proceedings. Provision of legal support to businesses and preparation of transactions listed in Art. 7.1 of the Federal Law "On Combating Money Laundering and Terrorist Financing" (engaging in real estate transactions; managing funds, securities or other property of the client; managing bank accounts or securities accounts; organization of contributions for the creation, operation or management of companies; and creation, operation or management of companies) are more typical of those providers of legal services who are not registered with the Bar.

Secondly, lawyers' chambers, legal practices and their branches themselves are not covered by AML/CTF regulations, because, being non-profit organizations, they are not allowed (with rare exceptions) to practice law on their own behalf or to engage in entrepreneurial activities.

In my opinion, these specifics should be communicated to our Western counterparts in the FATF mission, so that they, in assessing the effectiveness of our common efforts in the fight against ML/TF, can better understand its abilities as a member of the national AML/CFT system.

PROFESSIONAL ACCOUNTANT'S ETHICS CODE PROHIBITS THE PROVISION OF SERVICES TO A CUSTOMER GUILTY OF MONEY LAUNDERING

An interview with Evgenia Koposova, Director of the Russian Institute of Professional Accountants and Auditors (IPA)

Evgenia Koposova

FS: *Ms. Koposova, the IPA is the largest and one of the most respectable associations of accountants in Russia. What are its priorities?*

Evgenia Koposova: The IPA's priorities lie in providing practical and methodological assistance to its members in the field of accounting, defending occupational interests, setting occupational standards and representing the interests of accounting professionals at the national and international levels.

As an entity covered by non-state accounting regulations, the IPA is involved in the preparation of a program for the development of federal accounting standards; in the drafting, discussion and expert evaluation of the proposed concepts; and in the development of methodology guidelines in this area.

Membership in the IPA is voluntary. More than 350 000 accountants have been certified by the IPA since its establishment more than 20 years ago. The IPA network currently includes 63 regional associations of professional accountants and more than 400 training centres across Russia. About 70 000 professional accountants undergo skills upgrade trainings each year.

ИПБ РОССИИ
WWW.IPBR.ORG

FS: *How do you evaluate the AML/CFT knowledge of IPA participants?*

Evgenia Koposova: To enable the certification and professional development of accountants, the IPA has developed and maintains a system of knowledge- and skills-based requirements, compliance with which is tested in exams. They include the knowledge of the existing AML/CFT law. To test examinees' knowledge, we have developed a series of multi-level tests in the form of small case problems modelled upon real-life situations.

The knowledge of the relevant aspects of the AML/CFT law is included in the competitive tests of the traditional national contest for both practitioners and students "Russia's Best Accountant", which is held annually and has multiple categories.

IPA members (professional public and corporate accountants) are required to attend at least 40 hours (or 120 hours in three consecutive years) of professional development training per year. Some of them choose courses on internal or external controls with an integrated AML/CFT element. Training centres that use programs developed by the IPA, in addition to professional accountants, offer skill-upgrading courses also for other types of professionals, which broadens the range of accounting firm employees who are able to obtain information on this topic. In addition, the IPA posts all relevant AML/CFT documents on its website.

This year the Institute has signed a cooperation agreement with the International Training and Methodology Centre for Financial Monitoring. Under the agreement, our organizations will cooperate in preparing training, methodological, scientific, informational and analytical publications, holding joint conferences and workshops, as well as in assisting in the AML/CFT training, retraining and advanced training of personnel.

FS: *How do you ensure compliance by IPA members with AML/CFT requirements?*

Evgenia Koposova: Along with the requirement to attend annual skill-upgrading courses, IPA members must observe the Ethics Code for professional accountants. The Code sets out the key ethical principles and a conceptual approach to their observance, requiring all IPA members to refrain from participating in activities that have, or may have, a negative impact on the honesty, objectivity, and reputation of the accounting profession.

Thus, pursuant to Articles 3.15 and 3.16 of the Code of Ethics, any questionable characteristics of the customer, should they become known, may pose a threat to the honesty or professional conduct of a publicly practicing professional accountant. A list of such characteristics of a potential customer may include, among others, participation in illegal activities (money laundering and corrupt business practices).

INTERNATIONAL BLOCK

AREAS OF FATF FOCUS

The regular FATF Plenary Meeting took place in Paris on February 18-23, 2018. The main topics of the agenda included combating terrorist financing and new technologies

Alexey Petrenko,
Head of Rosfinmonitoring International Cooperation Department

Inessa Lisina,
Deputy editor-in-chief

Combating financing of terrorism remains one of the top priorities of the FATF global network over the last several years. In February 2016, following the terrorist attacks in Paris, the FATF adopted a consolidated strategy and an operational plan aimed at combating terrorist financing. Since then, the FATF has concentrated its efforts on identifying new and emerging terrorist threats, strengthening and refining its standards and assessing how countries implement necessary and effective measures to detect, prevent and punish cases of abuse of the financial system in support of terrorism. The FATF has achieved significant results in the four key areas identified in the 2016 operational plan.

To further enhance the international fight against terrorist financing, the Plenary has adopted a new action plan. This is a living document that provides a framework for a flexible and dynamic

response to terrorist financing risks. It is built on existing results and focuses on new areas which will increase understanding of the current risks and the effectiveness of measures to minimize these risks, while it is also flexible to address the continuously evolving threats. The said areas of increased focus include:

- further improvement of the identification and understanding of terrorist financing risks, both at country level and more broadly, which will have an impact on the effectiveness of international efforts to tackle terrorist financing;
- carrying forward the FATF's work to enhance information-sharing, which is based on the effort that FATF has already completed on inter-agency information exchange and exchange within the private sector;
- compilation of the best practices for identification of terrorist financing, *inter alia*, successful TF investigations, criminal prosecutions and convictions, including the initiative Mr. Santiago Otamendi, the FATF President, on increased engagement with the criminal justice system and judicial bodies;
- ensuring a better implementation of effective counter-terrorist financing measures through closer coordination with FATF style regional bodies and the actions they are taking.

The FATF will also continue to update information on the financing of ISIL, Al-Qaeda and affiliates.

The FATF Plenary adopted revisions to Recommendation 2. Now its requirements cover information sharing between competent authorities. It is emphasized that cooperation should include coordination with the relevant authorities to ensure the compatibility of AML/CFT requirements with data protection and privacy rules and other similar provisions (e.g. data security / localization). The integrated application of these requirements will facilitate exchange of information within the private sector.

These revisions are built on the modifications that have been introduced, at the last FATF Plenary, in the Methodology as it pertains to the information sharing requirements. Now, the updated Methodology and Recommendations are brought in line with each other. The revisions made in the Methodology will help assessors to analyze the extent of sharing information group-wide, including with branches and subsidiaries, and to understand whether or not sufficient safeguards are in place to ensure confidentiality and prevent tipping-off.

The Plenary adopted the updated FATF guidance on the implementation of financial provisions of the UN Security Council Resolutions to counter the proliferation of weapons of mass destruction. This paper will help countries to understand and implement these provisions, to ensure that targeted financial sanctions are implemented, and each country has effective mechanisms in place to prevent breaches. The guidance is available on the FATF website.

The Plenary FATF reviewed a report on the ML/TF risks associated with virtual currencies and the regulatory measures taken in this respect in different countries.

In November 2017, the FATF Plenary expressed its support for responsible financial innovation in line with the FATF Recommendations and for exploring its opportunities for more effective implementation of AML/CFT measures. Various work streams on FinTech and RegTech are currently underway as the FATF considers how its Standards apply in this context. The FATF Plenary heard presentations from some of its member countries concerning the initiatives in this area.

One of the key priorities under the Argentinean Presidency of the FATF is enhanced of engagement with national prosecution services and other stakeholders within criminal justice systems. The FATF President updated the Plenary on the outcomes of the second workshop for judges and prosecutors, organized in collaboration with the APG and EAG and hosted by China.

The Plenary also adopted the revisions to the High-Level Principles and Objectives for FATF and FATF Style Regional Bodies.[1] Now, this document contains new provisions pertaining to the principles of financial management of the FATF and FSRBs, including the following sections: source of funding; budget preparation, approval and management; and transparency and accountability. The updated document is available on the FATF website.

[1] The original document was adopted by the FATF Plenary in 2012.

The traditional meeting of the forum of the Heads of Financial Intelligence Units was held in the margins of the FATF Plenary. The participants discussed how to enhance the effectiveness of suspicious transaction reporting (STR) regimes and the quality of financial intelligence (including through the application of special IT tools). The participants shared their views on the importance of FIU autonomy and independence and its impact on the strategic and operational work of FIUs.

Since the private sector undoubtedly plays an important role in detecting suspicious transactions, *inter alia*, through filing STRs, the participants discussed the practical considerations in further developing public/private partnerships.

The strategic work performed by the FATF involves evaluation of the compliance of the national AML/CFT systems with the FATF Standards. The Plenary considered and discussed the mutual evaluation report of Iceland. The document is available on the FATF website.

The Plenary acknowledged the substantial progress made by Spain and Norway in improving their national AML/CFT systems since the adoption of their mutual evaluation reports in 2014. The Plenary agreed to re-rate a number of FATF Recommendations to reflect the current level of technical compliance of these countries.

The Plenary also discussed the progress of Brazil made in line with the action plan it agreed in November 2017.

The FATF congratulated Bosnia and Herzegovina for the significant progress in improving its national AML/CFT system and addressing the strategic AML/CFT deficiencies. Bosnia and Herzegovina will no longer be subject to the FATF's enhanced follow-up, and will work with MONEYVAL as it continues to further strengthen its national AML/CFT regime.

In June 2016, the FATF welcomed Iran's high-level political commitment to address its strategic AML/CFT deficiencies. Since November 2017, Iran has established a cash declaration regime and introduced draft amendments to its AML and CFT laws. However, Iran's action plan has now expired with a majority of the action items remaining incomplete.

Taking into account the steps taken by the country, it was decided to continue the suspension of counter-measures against Iran in November 2017. The FATF will make a decision on further steps in respect of Iran at the next FATF Plenary Meeting. It will be held in June 2018 in Paris, France.

"WE HOPE TO RESUME THE ROLE OF SYRIA IN THE INTERNATIONAL AML/CFT FIELD AS SOON AS POSSIBLE"

The Chairman of the Central Bank of Syria, Chairman of the AML/CFT Commission of the Syrian Arab Republic (FIU) Dr. Douraid Dergham answers the questions of the Financial Security Magazine

Douraid Dergham

FS: *The cooperation between Russia and Syria on the issues of establishment of the Syrian anti-money laundering system is carried out in the context of the war against "Islamic State". How effective is the exchange of information between our countries? In what format does it operate?*

Douraid Dergham: The exchange of information between Syria and Russia is fruitful in many ways, including, but not limited to enriching the data base, acknowledging the new adopted mechanism by the Russian FIU for tracing suspect transactions and enhancing the means of the Syrian FIU.

This cooperation has played a great role in developing, enhancing, and fastening the procedures taken from both countries to prevent the financial transaction that aims to finance ISIL in our region through the banking and the financial system.

FS: *Have you undertaken the analysis and monitoring of bank departments, the systems of cross-border and internal payments in current conditions as part of bilateral cooperation on sanitization of the financial and banking sector?*

Douraid Dergham: The cooperation between Rosfinmonitoring and the Syrian FIU was clearer in the field of finding the links between financial institutions which operate in the hot spot controlled by terrorists or within the neighboring countries and the Syrian jurisdiction. This has helped both FIUs to conduct a financial investigation on suspicious transactions passed from the mentioned area to the Syrian territories and detecting and suppressing such transactions.

FS: *In 2016 the new format of cooperation in combating the financing of ISIL was established with the participation of FIUs of Russia, Iraq, Iran and Syria, aimed to consolidate the efforts of these countries to prepare the evidential base of involvement of concrete financial institutions, business structures, non-profit organizations, intermediary countries and the UBO in "terrorist business". How could you evaluate the results achieved in this matter?*

Douraid Dergham: The four-lateral coalition is considered as a channel for the dissemination and sharing of financial and intelligent information about suspects involved in terrorist /terrorist financing crimes between the members of the coalition.

This coalition has raised the level of cooperation and coordination between the FIUs in these countries, and highly contributed in developing their abilities to collect, supervise, analyze, and exchange information of an important number of suspicious transactions that aims to finance ISIL and other terrorist groups. However, the coalition develops continuously its methods of cooperation in accordance with the new risks and challenges.

Working Group of FIUs of the Russian Federation, Syrian Arab Republic, Republic of Iraq and Islamic Republic of Iran

Proceeding from need to solve tasks of identification of channels and suppression of ISIL funding centers activity, in 2016, a working group of financial intelligence units of Russia, Iran, Iraq and Syria was established. The purpose of this working group is to coordinate the activities and the development of common methodologies and approaches to countering the financing of terrorism, as well as the formation of evidence base of involvement of specific financial institutions, commercial structures, NPOs indicating the countries of origin of financial flows, intermediary countries and the ultimate beneficiaries of the "terrorist business".

During this time, the working group has undertaken a number of comprehensive measures in the framework of a joint operation to counter the financing of terrorism, including:

- definition of terrorist activity zones (ZTA) as well as corridors, through which the penetration of foreign terrorist fighters in ZTA is organized, used as accessory bases, including for financial support of terrorists;
- identification and receipt of information from credit institutions, providing banking services to individuals and legal entities, including from the territory of the operation participants, etc.

Members of the working group conducted a capacity assessment of the national CFT systems in the context of works on detection, suppression and obstruction of operations with high terrorist risk.

As part of the interaction within the working group, a channel has been created and successfully operates to share information, including lists of persons involved in terrorist activities and designated operations involving such persons.

FS: *How could you estimate the assistance of Russia in AML/FT?*

Douraid Dergham: This cooperation was a good opportunity to exchange information between the two units, to support the Syrian efforts at the international level, and to highlight the role played by Syria in terms of AML/FT.

FS: *How could you estimate the experience of cooperation between our countries in the matters of specialist training for the emerging AML/FT system?*

Douraid Dergham: The training provided by the Russian Financial Investigation Unit to the employees of the Syrian FIU helped to improve the capabilities of the staff and to increase their skills in terms of financial analysis and electronic tracking methods. The training also helped to get acquainted with the Russian experience, especially on the issue of delisting.

FS: *How do you see the future of Syria on the thematic international platforms, such as FATF?*

Douraid Dergham: The Syrian FIU was always present at the international level to combat money laundering and the financing of terrorism, especially within the MENAFATF Group. Syria was one of the founding countries of the Group in November 2004, and participated actively in the joint assessment and technical teams. It is one of the first countries in the Middle East to be a member of the Egmont Group in May 2007.

However, the Syrian crisis, and the ways that some countries have taken to deal with Syria on a political basis rather than on a technical one have affected the contribution of Syria to the international scene. We hope to resume our role sooner.

FS: *What are the short-term plans of the Syrian FIU? What main goals and objectives do you set for the FIU of your country and in general for the country?*

Douraid Dergham: The short term plans of the Syrian FIU are concentrating on:

- building a comprehensive and accurate database and linking it with other national databases;
- focusing on training, increasing the skills of employees, and providing them with the necessary technical and analytical tools;
- continuing the mutual efforts made by the Syrian FIU, the competent authorities and the counterpart FIUs, in particular the Russian FIU to be delisted from the FATF's grey list.

The FIU also pursues its long-term plans, which aim to:

- review the legal and regulatory framework and introduce the required amendments that help the Syrian FIU to improve its performance and contribute effectively to the regional and international efforts devoted to fortifying the financial and banking system against suspicious operations, whether related to money laundering or terrorist financing;
- resume its role on the international level, through continuous and effective participation in the meetings and conferences of international groups and organizations, and overcome the obstacles that prevent its participation, for non-professional and objective criteria.

"WE ARE KEEN TO STUDY RUSSIAN FIU'S ACHIEVEMENTS"

An interview with Ahmad Heydarian, Deputy Head of the Iranian Embassy in the Russian Federation

Ahmad Heydarian

FS: *What is the state of AML/CFT cooperation between our countries?*

Ahmad Heydarian: Unfortunately, I must remind everyone of the tough geopolitical conditions we are currently living in, and that a lot of what the Western media tell people about Iran is untrue. Basically it is more about politics than about justice or truth.

Just recall the story of the Joint Comprehensive Plan of Action (JCPOA) on the Iranian nuclear program and the US behaviour. Can you imagine a country where after election the new head of state reneges on the agreements entered into by his predecessor? Or look at Syria and the things that are happening there today.

ISIL is indeed an international threat to the whole world. The US, having lived through 9/11 and knowing well what terrorism really means, has built an international coalition that includes several dozen countries.

But in reality, only Iran and Russia are fighting terrorism. I remember that a few years ago one of the State Duma deputies said that Iran is a wall between terrorism and Russia, and that without this obstacle it would have been much harder for your country to counter not only this threat but also drug trafficking.

Fortunately, cooperation between our countries, including on security issues, is now at the highest level ever.

I would also like to highlight our work on the ground in Syria. Cooperation between Iran and Russia is key to stability in the region. Our relations with Iraq, meanwhile, are also progressing. Thanks to Russia, Turkey has also been drawn into the process of finding solutions to the conflict in Syria, rendering the tripartite cooperation format between Iran, Russia and Turkey the most successful for Syria.

With respect to the fight against dirty money, including within the FATF framework, Iran has been working closely with Russia on this problem for the last 7-8 years. We have also met many times at Rosfinmonitoring, not only to discuss problems, but also to share information and experience. In fact, we are very keen to study Rosfinmonitoring's achievements.

FS: *What do you think about Iran's participation in the Financial Action Task Force on Money Laundering (FATF)?*

Ahmad Heydarian: With respect to Iran's participation in the FATF, we discussed this issue with Russia on numerous occasions. Russia is our neighbour, and we believe in the sincerity of your aid. We have a long way to go, but much has already been done. Whatever they say, we have some amazing results!

We try to be compliant with international AML/CFT standards, and this opens up new horizons for us. Iranian banks are ready to work hand in hand with financial institutions of other countries. But there are many more pitfalls for Iran, which are frequently discovered in the process of our cooperation with the FATF. It is highly unfortunate that Iran often becomes a hostage to politics and the target of Western prejudice.

Background

In February 2016, Rosfinmonitoring hosted a meeting of FIU Heads from Russia, Iraq, Iran and Syria, dedicated to strengthening cooperation in the fight against terrorist financing. The meeting was part of the international efforts to combat ISIL.

Meeting participants praised Russia for its efforts aimed at detecting and disrupting terrorist financing channels and centres used by Islamic State. The discussion focused on coordination of activities and development of common approaches to combating terrorist financing by the FIUs of Russia, Iraq, Iran and Syria.

On the side-lines of the meeting, Rosfinmonitoring signed bilateral information sharing agreements with the FIUs of Syria and Iraq.

EGMONT GROUP IS THE FATF STRATEGIC PARTNER

On March 11-15, 2018, the scheduled meeting of the Egmont Working Groups was held in Buenos Aires, Argentina. According to the Secretariat 319 representatives of different delegations took part in this event

Inessa Lisina,
Deputy editor-in-chief

The FATF President, Mr. Santiago Otamendi of Argentina, took part in the opening meeting and emphasized in his welcoming remarks the importance of the work performed by the Egmont Group. At present, both organizations face the common challenges and, therefore, use similar countermeasures to address them. Combating the financing of terrorism remains the key priority of the global AML/CFT system as well as for the majority of FIUs. In this context, it was natural that the Egmont Group was defined as the strategic partner in the FATF's new Counter-Terrorist Financing Operational Plan adopted by the FATF Plenary held in February 2018 in Paris.

The meeting was the first one chaired by Mrs. Hennie Verbeek-Kusters of the Netherlands. In her address to the delegates, she thanked Mr. Otamendi for active cooperation and bringing the positions of the FATF and the Egmont Group closer. Currently, the two organizations are implementing the joint project which involves analysis risks of misuse of corporate vehicles, legal arrangements and professional intermediaries.

At the previous Egmont meeting in Macau, the Head of the Argentinian FIU and Vice-Chair of the Egmont Group, Mr. Mariano Federici, proposed to focus efforts on addressing the money laundering of corruption proceeds. All working and regional groups submitted their proposals for potential discussion at the meeting. In particular, the Information Exchange Working Group compiled the list of corruption activities-related indicators based on the practical experience of the FIUs. These indicators include, *inter alia*, use of front companies, existence of single ultimate owner of several subcontractors, overpricing of delivered goods or services, use of alternative money transfer systems like hawala, etc.

The meeting of the Heads of FIUs adopted three anti-corruption initiatives, which highlighted:

1. Importance of operational autonomy and independence of FIUs;

2. Strategic importance of cooperation at domestic and international levels;

3. Priority of engagement with the private sector.

Other key projects and areas of research of the Egmont Group include virtual currencies, beneficial ownership, improvement of suspicious transaction reporting regime, combating the financing of terrorism and human trafficking.

For further strengthening coordination between the FATF and the Egmont Group, the Policy and Procedures Working Group, acting on instructions of the Egmont Committee, started in May 2016, to explore potential ways of cooperation between the two organizations for assisting FIUs in course of mutual evaluations. Assessment of the member FIUs for compliance with the Egmont requirements will now take into account assessment of effectiveness in achieving Immediate Outcome 2 (international cooperation) and 6 (use of financial intelligence for money laundering and terrorist financing investigations) in the framework of the FATF and FSRBs mutual evaluations.

The Egmont Group Center for FIU Excellence and Leadership (ECOFEL) started work in April 2018. Its main functions include mentoring activities, assistance to FIUs, exchange of experts and creation of an electronic library containing the relevant AML/CFT information and materials.

The 8th Best Egmont Case Award (BECA) competition will also started in April. The World Bank-UNODC Stolen Asset Recovery Initiative (StAR) will present a StAR Award of Excellence for the second time. The winners of the competition will be determined at the next Plenary Meeting in September 2018. The Technical Assistance and Training Working Group, responsible for running this competition, plans to start preparing the second compilation which will contain the best cases submitted for the competition in 2014-2017, with the focus on TF cases.

Wrapping up the meeting, Mrs. Hennie Verbeek-Kusters noted that, during this week, the delegates found new models of cooperation; discussed, in a coordinated manner, issues included in the agenda; achieved practical results; and adopted concrete decisions.

The Egmont Group meeting also issued the communique` in which the Egmont members and the international observers reaffirmed their commitment to combat corruption. This work will support the anti-corruption efforts of the FATF, FSRBs, G-20 and UN.

INTERAGENCY WORKING GROUP ON COMBATING ILLEGAL FINANCIAL TRANSACTIONS

AML/CFT KNOWLEDGE NEEDS TO BE HARMONISED

At its meeting on March 27, 2018, the Interagency Working Group on Combating Illegal Financial Transactions, chaired by E. Shkolov, assistant to the President of the Russian Federation, considered Rosfinmonitoring's initiative to facilitate interagency cooperation in the training of AML/CFT personnel. In particular, participants discussed the opportunities for cooperation between the network AML/CFT Institute and subordinate educational and scientific organizations in organizing personnel training and retraining, conducting joint research, etc.

Vladimir Ovchinnikov,
Director of the International Network AML/CFT Institute

In his address to the Federal Assembly, Russian President Vladimir Putin stressed that, in order to further restructure the Russian economy, we need to boost labour productivity on a new technological, managerial and personnel basis. Investments in infrastructure, education, technology and science should all work towards one strategic goal – a breakthrough economic development of Russia.

The issue of AML/CFT personnel training has remained relevant ever since the establishment of the Federal Financial Monitoring Service. Back then, 16 years ago, among the first to join Rosfinmonitoring were predominantly representatives of law enforcement agencies and the financial sector, to whom fell the task of building the country's AML/CFT system from the ground up. It was then that the need for AML/CFT knowledge harmonization became apparent. This led to the establishment in 2005 by the Russian Government of the International Training and Methodology Centre for Financial Monitoring, whose retraining courses were attended by several hundred employees involved in the fight against illegal financial transactions each year.

The actual number of employees currently working in the Russian AML/CFT system stands at over 120,000, all of whom must have the skills needed to combat illegal financial transactions. Given that it is not possible to train or retrain so many people in a single educational institution, Rosfinmonitoring, 5 years ago, decided to establish a network AML/CFT Institute, which brings together several Russian universities under the motto of training personnel for the Russian AML/CFT system.

The purpose of the network AML/CFT Institute was to create a common AML/CFT educational environment in the fields of IT, law, economics and finance, and international relations. Each of these universities currently has a department specializing in the training of personnel for the AML/CFT system.

Today, the network AML/CFT Institute comprises 34 leading universities from Russia and its partners within the international AML/CFT framework.

In 2017 the network AML/CFT was joined by five universities from Uzbekistan, two universities from Tajikistan and the China Centre for Anti-Money Laundering Studies of Fudan University, which is ranked 47th among the world top universities.

In 2017, the activities of the network AML/CFT Institute were focused on the following:

- training of AML/CFT personnel;
- creation of a common educational environment and provision of specialized training and methodological support;
- development and implementation of new specialized programs, methods and approaches to the training of personnel for national AML/CFT systems;
- promotion of Russian education abroad and development of international programs and projects.

Rosfinmonitoring's network AML/CFT Institute has won international recognition, becoming in 2016 the CIS leading AML/CFT educational and science centre and in 2017 a member of the UNCTC Global Counter-Terrorism Research Network.

The network AML/CFT Institute continues to expand the practice of open defence of thesis by its graduates before the professional community and employees of Rosfinmonitoring and its regional offices. In 2017 the master's degree in AML/CFT was awarded to over 220 network AML/CFT Institute graduates.

The network AML/CFT Institute, jointly with the Ministry of Education and Science, the Ministry of Foreign Affairs and Rossotrudnichestvo, continues its work on the international project to train foreign students at the universities of the network AML/CFT Institute: over 300 students from 21 countries currently undergo training at Russian universities.

Among the new study programs offered by participating universities in 2017 are "Financial Monitoring", "Financial Investigations in Organizations", "Legal Support of Economic Security in the Field of AML/CFT", "Compliance Control in the Activities of Economic Entities", "Information Support for Financial Monitoring", "Digital Economy", etc.

The network AML/CFT Institute's integrated research program "Mathematical and Socio-Economic Modelling for Anti-Money Laundering and Terrorist Financing", was endorsed by Russian President Vladimir Putin and is implemented by the institutes of the Russian Academy of Sciences. The Interagency Council, which is tasked with the implementation of this program, has been set up at the Federal Agency of Scientific Organizations. The Council is chaired by Viktor Zubkov, Doctor of Economics and the first Director of Rosfinmonitoring.

The goals of Russia's cooperation with its partners and Rosfinmonitoring's participation in international AML/CFT organizations are set out in the network AML/CFT Institute Action Plan 2018. They include:

- combining the efforts of the network AML/CFT Institute participants in support and promotion of Russia's initiative to establish a project team for technical assistance, education and science within the structure of the FATF Global Network Coordination Group; and
- promoting cooperation between Russia and China in creating a common AML/CFT educational environment in Eurasia and a CIS system of independent assessment of the qualifications of AML/CFT personnel.

One of the network AML/CFT Institute's focus areas is the provision of advanced AML/CFT training for the employees of law enforcement and supervisory bodies.

The International Training and Methodology Centre for Financial Monitoring is acting as the coordinator. In 2017, more than 800 law enforcement officers attended advanced AML/CFT training courses provided by the network AML/CFT Institute. Among the network AML/CFT Institute's partners in providing retraining courses were the following: the Investigative Committee Academy, the FSB Academy and the educational institutions of the Interior Ministry.

In addition to the retraining of law enforcement officers, training was provided in 2017 to more than 500 employees of supervisory bodies, including in cooperation with the Bank of Russia, the Federal Tax Service, the Assay Office and Roskomnadzor.

Far from being limited to Moscow and its region, Rosfinmonitoring's retraining efforts are focused on promoting cooperation between its regional offices and the regional universities of the network AML/CFT Institute.

Here is the most recent example. The need to develop a common approach to the training of students of higher education institutions of the Southern Federal District in combating illegal financial transactions was discussed on February 28, 2018 at an enlarged meeting of the Interagency Working Group on Combating Illegal Financial Transactions in the Southern Federal District. The meeting, held at the Rostov State University of Economics, a member of the network AML/CFT Institute, was chaired by Vladimir Gurba, Deputy Plenipotentiary Representative of Russian President in the Siberian Federal District.

Russia is currently undergoing an assessment of its AML/CFT system's compliance with the FATF requirements, which will be completed next year. Rosfinmonitoring has launched a large-scale training program for the personnel involved in the assessment. But the process of preparing the country will not be complete without the joint efforts of all affiliated educational institutions, which will help involve in the retraining of law enforcement and supervisory personnel a broad spectrum of professionals in the fight against illegal financial transactions.

In the work to combine the efforts of subordinated universities and educational centres and Rosfinmonitoring's network AML/CFT Institute, the focus should be on promoting cooperation between subordinated educational and scientific institutions and the network AML/CFT Institute in training and retraining personnel, conducting joint research, developing guidelines, etc. There is also a need for a joint interagency advisory body for the training of personnel specializing in the fight against illegal financial transactions.

TREND

ON LEGAL REGULATION OF NEW FINANCIAL TECHNOLOGIES

First international legal forum "CryptoSreda" was held in Moscow on March 1-2, 2018. The forum was arranged jointly by Vnesheconombank's Blockchain Competences Centre (hereinafter "the Centre") and the National University of Science and Technology "MISIS". The moderator was Elina Sidorenko, Head of the State Duma Working Group on Cryptocurrency Circulation Risk Assessment

Inessa Lisina,
Deputy editor-in-chief

The Centre, opened in December 2017, became the first expert organization in Russia to work on the integration of blockchain technology into the public administration sector, bringing together leading international experts and Russian practitioners specializing in the implementation of blockchain pilot projects.

A total of 30 speakers presented their views at the forum on the topical issues of practical regulation of new financial technologies, including cryptocurrencies. One of them was Pavel Livadnyy, State Secretary - Deputy Director of the Federal Financial Monitoring. In his speech, Mr. Livadnyy spoke about the risks linked to the abuse of cryptocurrencies and ways to mitigate them by legal means.

There can be no doubt that interest in new technologies, including FinTech (financial technology), RegTech (regulatory technology) and SupTech (supervisory technology), is growing around the world, with the global AML/CFT community being no exception. However, despite the impact such technologies have on the high-risk sectors, we are yet to move beyond the point of discussing the ways to regulate and mitigate the risks posed by them. That said, this situation is typical not only for Russia, but also for other jurisdictions and international organizations. This, however, does not mean that this sphere cannot be regulated – all illegal actions are covered by the relevant provisions of criminal law.

China's experience in regulating new technologies is a good case. It all began with enthusiastic attempts to legitimize such technologies, including, for example, through the state acquisition of stakes in mining farms, but ended in a ban. The reason is the high risk posed by new payment instruments.

According to Pavel Livadnyy, all payment instruments (which include more than cryptocurrencies) can be broken down into three main categories:

1. payment instruments similar to Bitcoin, which are not backed by anything and therefore highly volatile;

2. payment instruments similar to Ethereum, which are backed by their generating capacities; these categories are both tangible and tradable;

3. and finally, there are entities that are described in the Russian Finance Ministry's draft law as tokens. These are investment funds that are issued by existing business entities in order to attract additional investment.

Cryptocurrency trading platforms accept all three aforementioned new payment instruments without asking too many questions about their origin, which is something regulators see as potentially high risk that needs to be regulated like the banking sector.

The key principle of financial monitoring as laid down in the AML/CFT legislation is transparency in the activities of economic entities, achieved through the identification of customers, determination of their ownership structure and beneficial owners.

According to Mr. Livadnyy, we should not expect the emergence of unexpected regulations governing the activities of new financial market participants. From the point of view of financial intelligence, the regulation of their activities should include some elements of the fight against money laundering and terrorist financing, definition of the status of cryptocurrency trading platforms and other intermediaries, and determination of liability for failure to fulfil their financial monitoring responsibilities. All these steps should be based on the identification of users by financial service providers and submission of suspicious transaction reports to the designated authority. That is, these are the steps that are being implemented by all reporting entities. Therefore, the basic principles of the national system for countering illegal financial activities are also applicable to its new players.

CONTEMPORARY THREATS POSED BY THE CRIMINAL USE OF CRYPTOCURRENCIES[1]

Denis Kunev,
Head of the Russian Investigative Committee's Chief Directorate of Procedural Controls, colonel of justice

Denis Kunev

The issues of legal regulation and oversight of digital currencies is ranked today among the most discussed topics both in the economic and legal sectors.

Possible use of cryptocurrencies is currently the subject of a full-scale debate in Russia in other countries as well such regulation is seen in many ways. We have to admit that today's approaches to defining the legal status of cryptocurrencies, their mining and circulation not just differ, they are exactly the opposite, ranging from the use of prohibitive measures to full legalization and incorporation of the relevant provisions into the national legislation and cryptocurrencies into the country's financial system.

This is largely due to the speed of developments in the crypto world, where each new day brings not only fresh opportunities for new technologies and their application in the public sector and business environment, but also many hitherto unknown threats and challenges associated with the use of cryptocurrencies by unscrupulous market participants.

[1] The opinions expressed in this article are that of an expert, and do not represent the official position of the Russian Investigative Committee.

Today, depending on the jurisdiction, digital currencies are treated under domestic law as money, goods, payment/financial instruments, property. Their status in some countries, such as the United States, is determined in accordance with the court rulings adopted in a given state due to the peculiarities of the Anglo-Saxon legal system. Japan recognized cryptocurrencies as a legal payment instrument in 2017, China at the same time banned initial coin offerings (ICO) and related trading platforms. In Switzerland, as the country continues to draft the necessary regulatory framework, cryptocurrencies have already acquired the status of money in the real sector of the economy. Belarus, meanwhile, has already passed a decree "On the Development of Digital Economy", granting its citizens the right to freely receive, sell or buy cryptocurrencies without obtaining a special license or paying any taxes. In Russia several laws introducing the relevant terminology have been drafted.

Against the background of legal uncertainty, the number of crimes committed with the help of bitcoins and other cryptocurrencies – whose number has already exceeded 500 – is growing. According to some experts, the popularity and value of bitcoin was driven solely by the possibility to use information and communication technologies to conceal criminal activities. For example, at the APEC meeting on asset recovery, held in March 2018 in Bangkok, Thailand, attended by representatives of law enforcement and anti-corruption agencies, the phenomenon of cryptocurrencies was described as one of the contemporary threats and a major source of concern to the competent authorities of many countries around the world.

Law enforcement authorities, particularly in the states where the use of blockchain technology and digital currencies is no longer viewed as something unusual, regularly encounter offences whose sheer number allows their categorization into several distinct groups.

The first group includes the earliest type of cybercrime offences, which allow criminals to commit theft, extortion and other unlawful activities against both cryptocurrency holders and those who only intend to acquire them or use in other transactions. It may also include DDoS attacks on ICO platforms, whose aim is to steal cryptocurrency or disrupt the operations of a trading platform with a view of receiving a ransom. Therefore, it is clear that in countries where cryptocurrency trading is anonymous and outside the regulatory framework, it is much harder – if not downright impossible – to receive adequate law enforcement protection due to the absence of the subject of crime. A list of those affected may also include private persons who, for example, may be unware that their home or office computers have been compromised to mine cryptocurrencies.

The second group of offences becoming more and more common includes illegal transactions associated with the sale of restricted or banned goods or services in exchange for cryptocurrency. These include illegal trafficking in narcotic and psychotropic substances, weapons, human beings, sexual services, child pornography and stolen cultural values, etc.

For example, according to the UN World Drug Report, more than 25% of the world's drugs in 2016 were purchased over the Internet.[2]

The number of reports on technical shortcomings found in the blockchain technology itself, which allows users to store illegal information, is increasing. For example, back in 2015, at the Black Hat Asia conference in Singapore, investigators working with Interpol stated that they could embed illegal content – including malicious software – in the so-called free sectors inside the bitcoin distributed ledger[3]. No specific approaches to removing this data has been proposed so far.

At the same time, law enforcement authorities in different countries in large part have already perfected the techniques used to investigate illicit trafficking in banned items and services, culminating in several convictions. For example, the notorious case of the anonymous Silk Way trading platform creator Ross William Ulbricht. The marketplace trade volume generated some 9.5 million bitcoins and exceeded $80 million in commissions. Following his trial in 2015, Ulbricht was sentenced to life imprisonment on charges of trafficking in banned items, committing cybercrimes and money laundering. In another case, in 2017, one of the

[2] http://www.unodc.org/doc/wdr2016/WORLD_DRUG_REPORT_2016_web.pdf.

[3] https://www.darkreading.com/black-hat/black-hat-asia-2015-money-talks/d/d-id/1319016.

operators of the now-defunct bitcoin exchange Coin.mx was sentenced to 16 months in prison. In the Netherlands, last year, during a police inspection on online marketplaces, investigators arrested 10 people for attempting to sell bitcoins generated from the sale of drugs through a network of intermediaries. In Denmark, a resident of the kingdom was sentenced to 8 years in prison for engaging in similar illegal activities. Similar criminal investigations have been launched by Russian law enforcement authorities, underscoring the urgency of the efforts aimed at identifying and responding to emerging risks, as well as at having a clear understanding of the threats posed by the new virtual reality.

Meanwhile, the use of cryptocurrencies for money laundering and terrorist financing is increasing, at least according to the Financial Action Task Force (FATF) reports. The FATF following its February 2018 Plenary meeting, decided to adopt additional initiatives to minimize the risks associated with cryptocurrencies[4].

Only a few years ago, prior to the launch of successful investigations by some countries, crimes committed with the help of bitcoins were routinely compared to a chain of clandestine activities that – thanks to the anonymous nature of transactions – prevented the identification of the perpetrators. Today, however, there can almost be no doubt that it is the blockchain technology itself that guarantees that the crime will be solved and all anonymous users will be found. And therein lies a certain paradox of cryptocurrencies. Transactions with their use leave an indelible forensic trail that makes any hidden financial history public in a matter of minutes. The success of each given investigation depends on the skills and knowledge of financial intelligence and law enforcement officers, as well as on the technological tools available to them, such as special software programs for tracking illegal financial flows. At the same time, law enforcement agencies of many countries call for the creation of a common database of cryptocurrency users, the use of a more coordinated approach to joint investigations and the establishment of an appropriate regulatory framework.

A major role in providing methodological support for ongoing investigations is played by the United Nations Office on Drugs and Crime, which declared that digital currencies are more frequently used to commit crimes. Therefore the organization developed a special training course on cryptocurrency investigations and offers annual trainings for the personnel of law enforcement and financial intelligence agencies.

The steady growth in the number of crimes committed with the help digital currencies, coupled with individuals' vulnerability to such attacks, underscores the need for legal regulation and control of cryptocurrencies in order to determine their legal status. At the same time, it is extremely important for countries to apply a common approach to such regulation, a task impossible to achieve without the development and adoption of a universal international legal instrument setting out not only the legal status of a cryptocurrency, but also the framework standards for its circulation, including unified ML/TF requirements.

It seems that until the world community comes to a consensus on these and a number of other issues of legal regulation of cryptocurrencies, private individuals, businesses and the government will continue to face the prospect of criminal manifestations, the likelihood of which should be taken into account in any transactions when building a digital economy. However, this should not be seen as an obstacle to the continuation of dialogue and constructive engagement in this area between law enforcement and financial intelligence agencies around the world.

[4] www.fatf-gafi.org/publications/fatfgeneral/documents/outcomes-plenary-february-2018.html.

AML/CFT TRAINING

Today professional development training of private sector representatives becomes especially important and relevant for the national AML/CFT system. These efforts should ensure sustainable development and transparency of the financial system of the Russian Federation

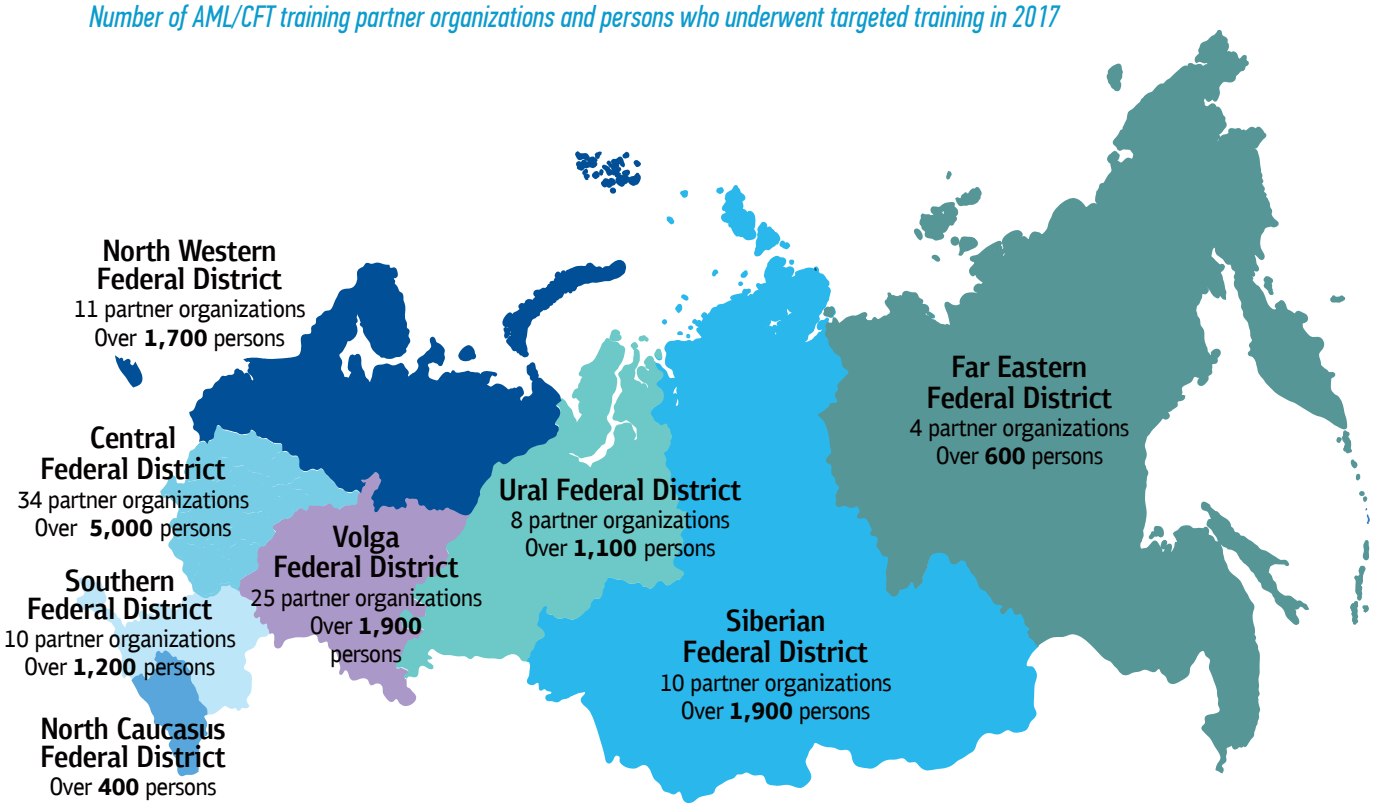
Ekaterina Avaeva,
Advisor of Education Department,
International Training and Methodology Center for Financial Monitoring

The International Training and Methodology Centre for Financial Monitoring (ITMCFM) enters into cooperation agreements with educational institutions and other organizations (partner organizations) involved in provision of AML/CFT training. The Centre keeps integrated records of persons who undergo training under the targeted training program and maintains the register of issued training certificates.

The ITMCFM partner organizations include multidisciplinary training centers, educational institutions specialized in training of certain types of entities covered by the AML/CFT legislation and universities, including the members of the International Network AML/CFT Institute (Peter the Great St. Petersburg Polytechnic University, Rostov State University of Economics, Lobachevsky State University of Nizhny Novgorod).

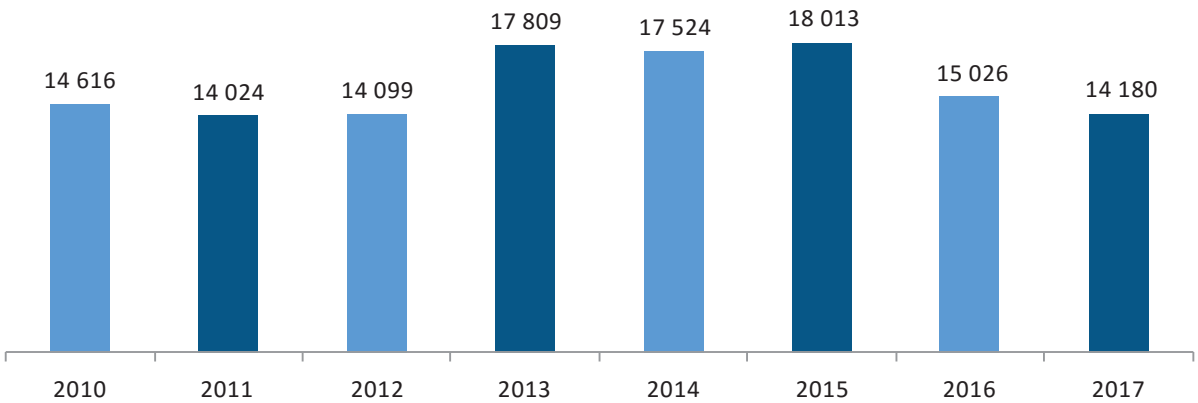
The established network of educational institutions than implement AML/CFT training programs allows for training annually over 14,000 employees of business entities engaged in transactions with funds or other assets.

Number of AML/CFT training partner organizations and persons who underwent targeted training in 2017

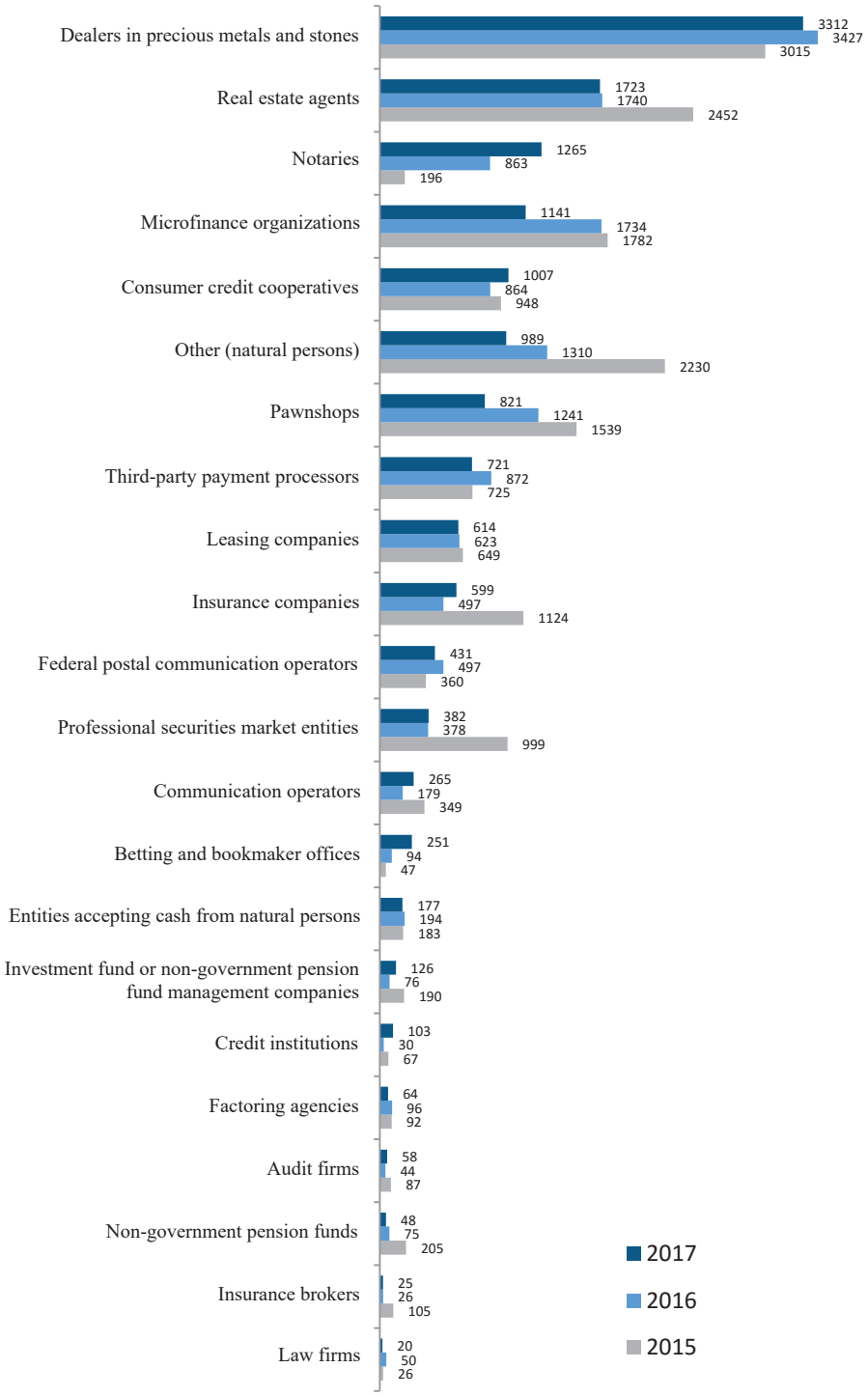


In 2010-2017, more than 130,000 private sector specialists participated in AML/CFT targeted training. Continuous engagement of new business entities carrying out transactions with funds or other assets in the training process enables to improve compliance with the international requirements and mitigate ML/TF-related risks. In particular, to promote more active involvement of DNFBPs in the AML/CFT efforts and to enhance effectiveness of preventive measures applied under the internal control systems, the program of regular training of notaries has been developed and is implemented at the training center established by the Federal Notarial Chamber. In 2017, over 1,200 notaries took part in trainings, and more than 2,400 notaries underwent professional development training courses.

Number of employees of business entities and individual entrepreneurs involved in transactions with funds or other assets who attended targeted trainings in 2010-2017



Number of employees of business entities engaged in transactions with funds or other assets who underwent AML/CFT targeted trainings in 2015-2017 (broken down by types of entities/ activities)



The efforts to ensure and strengthen the national security require enhancement of the role and responsibility of both employees of entities that implement AML/CFT measures and personnel of AML/CFT training and educational institutions. The ITMCFM provides ongoing consultative and methodological support for AML/CFT education and training of staff.

SOCIAL SYSTEMS IN THE DIGITAL ECONOMY

A list of the latest global trends includes the development of digital information and communication technologies (DICT) and the immersion of humans into such technologies

Anatoly Kolesnik,
Adviser to VTB Bank, Doctor of Economics and Candidate of Technical Sciences

Anatoly Kolesnik

The global feature of this trend is manifested in the "digitalization of everything", a process otherwise known as the "digital economy". Russia is one of the countries to have declared its intention to build and develop the digital economy, as evidenced from the relevant program approved by the Russian Government (RG Decree No. 1632-r of July 28, 2017). In this Program, the digital economy is defined as "an economic activity whose key factor of production is digital data, and which contributes to the creation of information space with account for the needs of citizens and society in obtaining quality and reliable information; the development of the information infrastructure of the Russian Federation; the development and adoption of Russian information and telecommunication technologies; as well as to the establishment of a new technological basis for the social and economic sphere".

The Program focuses on the two lower levels of the digital economy, setting out the key goals and objectives of its development:

- key institutions responsible for the development of the digital economy (regulatory framework, human resources, education, development of research skills and technologies);
- basic infrastructure elements of the digital economy (information infrastructure and information security).

Given the DICT-related organizational and infrastructure constraints currently affecting the Program, we still have the opportunity to reflect on how digitalization can be implemented in the country's social sector, and how ordinary Russians can benefit from it.

From the economic theory perspective, the digital economy has emerged from the concept of "knowledge economy" – which began its active expansion around the world back in the 1960s – as the main content of the post-industrial economy. "The knowledge economy is an economy where growth is driven largely by knowledge and human capital. Its development depends on improvements in the quality of human capital and life, as well as in the production of knowledge, advanced technologies, innovation and high-quality services" (Wikipedia).

To date, the knowledge economy has been reduced to the digital information economy, although "human knowledge is not reducible to universal processes; i.e. it cannot be described, for example, solely in terms of information flows [10, p. 341]".

If the knowledge economy provides for an increased intellectual potential of the population, the digital economy, on the other hand, will dispose of the people employed in the economy, transforming the rest into the appendages of digital systems.

In the digital economy, the entire working population will be divided into the following four groups:

- those developing and producing digital technologies along with the modes of their application in the economic sectors;
- those maintaining the operation of digital technologies in the economy during their life cycle;
- those employed in the digital economy and working in tandem with digital systems as operators/appendages of these systems; and
- those who are about to lose/have lost their job due to the digitalization of the economy.

It is possible that the US promotion of universal digitization was linked to its efforts to create artificial intelligence (AI), which go hand in hand with its intensive research into the brain and human consciousness. After all, the US Congress allocated substantial resources for such research: The Brain Research through Advancing Innovative Neuroethologies (BRAIN).

This project was promoted by US President Barack Obama: "There's this enormous mystery waiting to be unlocked. The BRAIN Initiative will change that by giving scientists the tools they need to get a dynamic picture of the brain in action and better understand how we think and how we learn and how we remember".[1]

Some scientists, including from Russia, view the efforts to promote the creation of artificial intelligence with considerable concern: "Already today, the privately-held US start-up company Vicarious is working to build a digital model of the neocortex (a new artificial brain cortex) capable of sensory perception, conscious thinking and speech.

If they succeed, it will dramatically alter not only the labour market – by making redundant hundreds, or even billions, of people – but also humans themselves, reaching a point at which AI will turn humans into robots – or make them disappear altogether. The uncontrollable development of AI potentially poses a greater danger than nuclear weapons or any other modern challenges".[2]

[1] http://www.bbc.com/russian/science/2013/04/130402_brain_mapping_obama

[2] http://prointellekt.com/articles/rubrika-dolzhnost-i-nravstvennost?yclid=7233239145204161082

On November 9, 2015, the US Department of Commerce unveiled its digital economy agenda, consisting of the four major challenges:

- global and free Internet;
- trust and security on the web;
- access and skills;
- innovation and emerging technologies.

Expanding the topic of the digital economy, the US is seeking a free cross-border movement of information and the lifting of any regional restrictions on its storage and processing. To this end, it is running a pilot program to create in US trade offices around the world the posts of so-called digital attach s. In other words, we are talking about the US digital expansion into other countries. The efforts of the US and multinational companies in this are supported by the World Bank, which acts as one of the key promoters of the digital economy around the world. According to the information posted on the World Bank Group website[3], "developing the Digital Economy in Russia is the initiative of the World Bank and its partners from the Russian government, business entities, civil society institutions and the scientific and educational community".

To ensure that our experts continue to use their products[4], these companies organize workshops and other forums in Russia, convincing Russian engineers of the benefits of using certain products and technologies developed by Western/American multinationals[5]. To some extent, this is reminiscent of the efforts by IT companies to create and exploit the so-called problem Y2K, when, according to experts, a total of $300 billion was spent on preparing for the year 2000[6]. This expenditure was completely avoidable, as the author of this article learned from his own experience and that of one large federal agency. The level of expenditure on the digital economy is several orders of magnitude higher than on a solution to fix the Y2K problem. To generate the required funding around the world, the interested parties may well resort to consciousness manipulation. How this may happen is illustrated by the following quote: "The prominent ideologist of perestroika N. Amosov wrote: "Exact sciences will absorb psychology and the theory of knowledge, ethics and sociology, and, consequently, there will be no room for reasoning about the spirit, consciousness, universal reason and even about good and evil. Everything is measurable and manageable"" [5, p. 88].

However, the propagation of the ideas of the digital economy in the world may have other purposes. One of them assumes that multinationals will move away – many of them have already done so – from the strategy of expanding technologies developed in parent companies to the periphery, to adopt the strategy of absorbing new knowledge and technologies from external sources [8]. Naturally, the ubiquitous work (spearheaded by multinationals) on the development of the theory and practice of the digital economy will create new opportunities for such absorption, thereby making these companies even more powerful.

In the current situation, in order to remain competitive on the geopolitical stage, our country is "doomed" to develop its digital economy. To avoid ceding control over the digital economy to multinationals and those who stand behind them, however, we need to ensure crypto security of DICT, which is described in the approved "Russian Digital Economy" program as one of its key building blocks.

In addition, we need to "develop immunity" to the destructive effect of digitalization on people and social stability.

---

[3] http://www.vsemirnyjbank.org/ru/events/2016/12/20/developing-the-digital-economy-in-russia-international-seminar-1

[4] "Due to the degradation of our electronics industry and the widening development gap in the field of nano and information and communication technologies, it is not possible to replace imported equipment with own production in any significant number of product categories."

[5] In his book "Suggestion and Its Role", the renowned Russian scientist V M. Bekhterev examined in detail the process of suggestion; that is, the actual imposition of "one or other mental states" on another person: "...suggestion is nothing but an invasion of the mind or instilling in it an extraneous idea without the direct involvement in this act of the subject's self, as a result of which the latterin most cases is either completely or almost powerless to reject it and expel it from the sphere of consciousness, even if it realizes its absurdity". (https://www.litmir.me/data/Book/0/92000/92750/Behterev_Vladimir__Vnushenie_i_ego_rol_v_obshestvennoi_chizn Litmir.net_92750.fb2.zip)

[6] https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D0%B1%D0%BB%D0%B5%D0%BC%D0%B0_2000_%D0%B3%D0%BE%D0%B4%D0%B0

It seems that when it comes to the matters of digitalization, we need to consider society not as a machine, but rather as an organism, and to clarify how certain engineering solutions that are part of the digital economy will affect this organism now and in the future.

Let's consider what potential modifications could be introduced in the domestic social security (pension, social security insurance and health insurance) systems as part of the digital economy development process. Currently, funding of these social security programs in based on the insurance principles. The social security budgets depend on labor remuneration. Those who generate the relative fund flows (employers, other insurers and self-employed people) transfer part of this money, as per the statutory rates, for funding the three social security programs mentioned above. By monitoring the socially oriented fund flows, the State (government) exercises control to ensure that insurers make adequate and full contributions to these social funds. The ongoing digitization of money (introduction of crypto-currencies) is aimed at depriving the State of these controls[7], which will annihilate the social insurance mechanism. Apart from social insurance, the government control over the financial flows is also needed for the tax administration purposes.

Thus, the first restriction for further expansion of digital economy may be articulated as follows: any digitization processes, whatever they may be, should in no way result in loss of control over the financial flows by the State which guarantees funding of the social security programs. In other words, this commitment of the State should be supported in practice. This requires not just legislative actions, but also adequate response of the government authorities responsible for cash circulation (Russian Central Bank) and for administration of taxes and social insurance contributions (Federal Tax Service). Since the attack aimed at depriving the State of control over the fund flows is conducted with the application of digital information and communication technologies, the response should be focused mainly on these technologies. Quite possible that in order to "narrow the frontline of this confrontation" it would be expedient to abandon the existing insurance contribution system in favor of a new system where the social security programs will be funded from the State budget. In previous publications (e.g. [15]), the author argued that introduction of an insurance-based pension system is a mistake in a long term, therefore, transition to funding, for example, of the pension system from the government budgetary revenues will cause no serious shock.

These ideas can be illustrated by the following model of hypothetical interaction between an individual and a pension system in the "developed digital economy", as outlined below. Let's assume that the pension scheme remains the same as it is now (i.e. consists of savings and insurance contributions). An individual X will reach the mandatory retirement age soon. One month prior to the retirement date, he receives an e-mail or an SMS message stating that all individuals who will reach the mandatory retirement age next month should visit the (indicated) website/ portal to find out more about their rights and duties as retirees and to undergo the test for assessing their readiness (preparedness) to effectively exercise their pension rights.

Since the pension system databases contain all relevant (in terms of pension coverage) information about this individual (date of birth, place of employment (employment history, regional benefits), salary/income at each place of employment, accumulated pension capital), the message may be addressed specifically to such individual taking into account his employment history. Therefore, when he visits the recommended web portal of the pension system, he is provided not with full text of the laws and regulations, but only with those legislative provisions that are relevant for him personally. The test for assessing knowledge by an individual of his pension rights may include questions about documents needed for granting a pension and for adjustment of pension amount (for inflation and for employed retirees) as well as questions about methods of pension delivery, value of pension scheme scores, obligations and methods of on-going contact with the pension system, etc. This portal may also include online tools for selecting a new profession and new place of employment if a retiree cannot practice his "old" (previous) profession any more, but wishes and is capable of performing socially beneficial activities.

The pension portal may ask questions about those periods of individual's life, information on which is

[7] In her speech delivered at ITMO University, Natalya Kasperskaya, the president of InfoWatch and co-founder of Kaspersky Lab, stated that hiding behind the alleged inventor of bitcoin Satoshi Nakamoto is a "group of US cryptographers", and the crypto-currency itself was developed by the US secret services. (https://anycoin.news/2018/01/19/infowatch/)

missing in the pension system, or there are doubts about veracity of such information. After this, the search engines built in the pension system will try to find answers to the questions raised in respect of a given individual in the information systems of other organizations, and only if such information is not found, the portal will request the individual to visit the pension system office where the front-desk personnel will explain what documents should be obtained from his former employers, and how they should be submitted to the pension system, inter alia, by e-mail or via the web portal. Once these questions are clarified and full information on the pension rights and pension delivery methods is collected in the system, the individual will be requested to confirm and certify this information by his electronic signature or otherwise, after which the amount of pension will be calculated and communicated online to the individual.

After that, the system will take certain "time out", so that the pension agency can adopt the relevant decision, and the final information will be communicated to the individual by SMS message, e-mail or by other "digital" method. Thereafter, the system will inform the individual each time when his pension is delivered and request him to confirm the delivery.

If no such confirmation is received, the system will check whether the individual has left the country and initiate, if necessary, the inquiry by the relevant agencies to clarify why no feedback is received from the individual. It goes without saying that the pension system portal will inform the individual about meaningful and significant changes in the pension legislation and pension technologies. (For such information not to be excessive, it is advisable not just keep an individual updated about changes that affect him personally, but also give him the opportunity to read full text of laws and regulations that modify the established procedures).

In the context of digital communication between an individual and the pension system, the following principles should be adhered to:

- provided information should be relevant to particular individual, but full information should also be available to him, if he wishes so;
- if an individual does not read the information forwarded to him in the digital format, he should have the opportunity to get familiarized with such information via voice communication channels;
- if an individual wants to receive information not from a computer system, but by way of face-to-face contact with the staff, such opportunity should be granted to him in the most convenient and easiest manner. Digital information and communication technologies should not prevent people from visiting social organizations or from maintaining voice contacts via the communication (including digital) channels. In other words, DICT should not separate people, but facilitate human contacts.

There is one significant challenge in digitalization of the social environment (in this publication, the author will consider this problem only in the context of the pension system). It is commonly assumed that information on a particular individual contained in the government information systems is correct, adequate and constantly accessible, which is not always true. Any systemic errors in reporting documents or in interaction among the government information systems (e.g. tax and pension systems) may cause an avalanche of erroneous actions in the pension system computers, which, in turn, may lead to disastrous outcomes.

In light of deteriorating software design culture observed in recent years, this risk is quite real, particularly as the existing pension system includes non-government pension funds that manage large amounts of funds generated in the government pension system. Operation of non-government pension funds may involve potential ML/TF risks, as highlighted by the head of the Financial Market Committee of the State Duma Anatoly Aksakov.[8]

Therefore, the computer "back-office" of the pension system in the digital economy should be considered and treated separately.

[8] https://regnum.ru/news/2377725.html. "…the mandatory portion of pension contributions transferred to non-government pensions funds through the Pension Fund (6% of the pension rate) is legal and transparent, and no question arises as to who make these contributions. Thus, possible illegal origin of funds paid as insurance contributions is monitored by other government agencies. However, there is also the voluntary portion of contributions that people may potentially transfer for illegal purposes, e.g. for laundering criminal proceeds. These voluntary contributions should be scrutinized under the AML/CFT Law".

In terms of the applied algorithms, the requirements of the "back-office" are met by the currently used software until future changes in the federal pension legislation. There are two processes in the pension system for each individual. The first process involves keeping record of the indicators that determine the pension rights of an individual based on his/her socially useful activities (according to the insurance principle the "socially useful activities" involve only efforts aimed at earning money, which makes it spiritually inferior[9]). This process starts when an individual begins socially useful activities and continues throughout his life. The second process starts from the moment when pension is granted to an individual and involves calculation of amount of pension based on information collected under the first process by the time of retirement. The second process is also on-going and includes adjustment, indexation and recalculation of pension based on updated information about the pension rights and changes in the pension legislation.

For brevity, the first process is referred to as the process of recording information on pension rights; and the second – the process of adjustment of pension rights, payment of pension and other operations of the pension system[10]. The current IT development trends in our country lead to collection and storage of personal data of each citizen, including biometric data.

And finally, I would like to recall the commonly known fact that scientific and technological achievements may be used both for benefit of and harm to human beings. But today, when the human civilization is riven with discord, all government actions should be thoroughly elaborated such as to prevent harm.

REFERENCES:

1. Orekhov, V.D., Forecasting Human Development with Consideration for Knowledge Factor, Zhukovsky city: MIM LINK, 2015.
2. Bakhtiyarov, O., Active Consciousness, Moscow: RIPOL classic, 2015.
3. Glazyev, S., Great Digital Economy: Challenges and Prospects for the Economy of the 21st Century, http://ruskline.ru/opp/2017/sentyabr/14/velikaya_cifrovaya_ekonomika_vyzovy_i_perspektivy_dlya_ekonomiki_xxi_veka/.
4. Varkholova, T., Dubovitska, L., European Union Strategies: Focus on Competitiveness, *Scientific Dialogue*, Issue 1(37), 2015 (http://elar.rsvpu.ru/bitstream/123456789/15667/1/2015_37_007.pdf).
5. Kara-Murza, S., Manipulation of Consciousness, the XXI Century, Moscow: TD Algoritm, 2015.
6. Opening Speech of His Holiness Patriarch Kirill at the Meeting of the XXI World Russian People's Council (http://www.patriarcgia.ru/db/text/5052002.html).
7. Leontyev, K.N., Orient, Russia and Slavdom, Moscow: Respublika, 1996 (http://antimodern.ru/interview-2/).
8. Speech of His Holiness Patriarch Kirill at the Meeting of the Supervisory Board of "Alexander Nevsky" Program (http;//www/patriarchia.ru/db/text/3757984.html)
9. Mindeli, L.E., Pipiya, L.K., Conceptual Aspects of Development of Knowledge Economy (http://ecfor.ru/wp-content/uploads/2007/fp/3/10.pdf).
10. Social Philosophy of Science: Russian Prospects, Treatise, edited by Krasavin B.T., Correspondent Member of the Russian Academy of Science, Moscow: KRONUS, 2016.
11. Nazarchuk, A.V., Niklas Luhmann's Concept of Communication, Moscow: Ves Mir, 2012.
12. Katasonov, V. Understanding of Society from the Orthodox Christian Standpoint, Institute of Russian Civilization, Moscow: Institute of Russian Civilization, 2015.

[9] From the material perspective, the insurance-based pension system in our country creates risks to stability and facilitates disunion among people, as described by the author in publication [15]. Unsuitability of the insurance principles for pension coverage in our country may be illustrated by fact (confirmed by the legislation) that the amount of the current insurance pension may be lower than the minimum subsistence level.

[10] Hopefully, the pension system will also include measures aimed at satisfying the spiritual needs (e.g. communication needs) of retirees, and measures that would make it possible to use the social capital generated by retirees during their active life.

13. Platonov, O.O., On Metaphysics of the Russian World: Russian World Doctrine, Moscow: Izborsk Club, Knizhny Mir, 2016.

14. Under the Power of Inhumans: Will the Advantages of Digital Economy be Used for Benefit of Human Beings? / Argumenty b Fakty, No.52, 2017.

15. Kolesnik, A., Lessons Drawn from the Damage of the Russian Pension System Paradigm/ Business Strategies Online Magazine No.7, 2017. http://www.strategybusiness.ru/jour/article/view/341/310.

16. Klimets, A., Continuous Logical Thinking – Absolute Weapon. (http://re-tech.narod.ru/homo/psyhj/abslog.htm).

17. Malakhov, A., "Come on!", Anniversary Report of the Club of Rome. (http://malakhov.link/come-on-report)

VIDEOCONFERENCING

DATA ANALYSIS TECHNOLOGIES IN THE PUBLIC SECTOR

Konstantin Litvinov,
Editor-reviewer

On February 2, 2018, the International Training and Methodology Centre for Financial Monitoring (ITMCFM) hosted a workshop on "How to Receive Informative Reports from Banks". The issues related to the effective financial monitoring via videoconferencing were discussed jointly with the banking sector by concerned representatives of the public and private sectors from Belarus, Kazakhstan, Kyrgyzstan, Tajikistan and Uzbekistan. Russia in off-line regime was represented by the employees of Rosfinmonitoring, Rosselkhozbank, VTB Bank, Tinkoff Bank, Russian Capital Bank, TransFin-M, T2 Mobile, MTS, MegaFon and the Russian Post.

The role of the main speaker was assigned to Andrey Denisenko, an expert in developing analytical solutions to combating public sector fraud.

In his opening remarks, the speaker emphasized that the data analysis technologies that are already widely used in the banking sector may also be useful in the public sector, with the greatest benefit in terms of AML/CFT archived through their competent application and understanding of the banking sector's modus operandi.

The first part of the workshop included a discussion of the current situation in the relevant area and possible directions of AML/CFT development with respect to the submission of suspicious transaction reports (STRs). The speaker focused on the advantages and disadvantages of mandatory and internal controls, the issues related to the development of internal controls and the prospects for receiving more informative reports by financial intelligence units. A.Denisenko provided a detailed description of this working mechanism, including how to analyse incoming data and generate informative STRs.

In the second part of the workshop participants discussed how to use analytical processes in order to ensure that the system used to generate STRs for the FIU is effective and up to date. In particular, A.Denisenko spoke about the prospects for successful cooperation between the FIU and banks in combating terrorist financing, emphasizing the potential for identifying planned terrorist attacks solely with the help of primary financial monitoring.

In conclusion, participants thanked the speaker for the information provided, highlighting the potential of the outlined techniques and the need to continue research into this topic in order to ensure that financial intelligence units and bank staff are aware of the latest developments in approaches to banks' submission of STRs to the FIU.

COMBATING ANONYMITY IN DECENTRALIZED CRYPTOCURRENCIES

A workshop on "Decentralized cryptocurrencies and blockchain: underlying technology, ML/TF risks and mitigation measures" was held at ITMCFM on February 9, 2018. The speaker - Pavel Shust, Executive Director of the E-Money and Remittance Association (EMA)

Konstantin Litvinov,
Editor-reviewer

The workshop was attended via videoconference by representatives of Armenia, Belarus, Kazakhstan (Financial Academy of the Finance Ministry, a member of the network AML/CFT Institute), Kyrgyzstan, Tajikistan and the Institute of Financial and Economic Security MEPhI (Russia). Among Russian representatives attending the meeting in person were employees of Sberbank, Tinkoff Bank and Russian Capital bank.

The first part of the workshop focused on the history of electronic money, their evolution and development, the transition from a centralized to decentralized system, etc. In the second part, Pavel Shust turned his attention to the issues of cryptocurrency anonymity, ML risks and mitigation measures.

Originally, it was believed that decentralized cryptocurrencies provide anonymity, but today we understand that this is not the case: investigators can study the links between transactions and use other ecosystem participants for identification purposes. The problem of anonymity in decentralized cryptocurrencies is due to the absence of a central counterparty, which leaves authorities pursuing investigations, including into money laundering and terrorist financing, without a point of contact.

The speaker pointed out that customer identification typically occurs at the confluence of regulated and unregulated sectors, i.e. in exchange offices, various stock exchanges, etc. which is arguably the most appropriate approach to identifying decentralized system participants.

According to Pavel Shust, example of investigations into bitcoin transactions can be found, although they tend to differ from ordinary financial investigations due to their focus on the links between transactions. The difference is that in decentralized cryptocurrency systems, transactions are known while their parties are not (in centralized systems, it is the opposite: the parties are known while the transaction is not), hence investigators' focus on transaction analysis. The speaker showcased how such transactions are studied and how the generated knowledge helps in ML/TF investigations.

Summing up the lecture, Pavel Shust re-emphasized the existence of specific risks associated with cryptocurrencies, noting that this sector does not exist in isolation. Instead, it is connected to the regulated market, which means that risk mitigation mechanisms do exist: "*Decentralized cryptocurrencies may yet become common in the financial sector, meaning that regulators need to assess the risks and take mitigation action. International experience of using various identification mechanisms offers a wide range of options without the risk of non-compliance with the FATF Recommendations*".

Publisher

Autonomous Non-Profit Organization ITMCFM
Staromonetny Lane 31, bld.1,
Moscow, Russia, 119017. E-mail: info@mumcfm.ru.
Number of copies: 150.

Autonomous Non-Profit Organization ITMCFM

2018