Евразийская группа
по противодействию
легализации преступных доходов
и финансированию терроризма
www.eurasiangroup.org

EAG

Eurasian group on
combating money laundering
and financing of terrorism
www.eurasiangroup.org

№ 32 (SEPTEMBER 2017)

EAG BULLETIN

CHAIRMAN'S COLUMN

Dear colleagues!

The Eurasian Group has focused on the preparation and process of mutual evaluations, in which national AML/CFT systems are assessed for compliance with international standards. On the eve of the evaluation it is important that the EAG member states ensure timely collection of statistical data, and develop constructive interaction with all participants of the national AML/CFT systems. Evaluation of effectiveness will also focus on effectiveness, therefore it is necessary to work with prosecutors and judges as they are responsible for enforcement of AML/CFT measures.

During the 27th EAG Plenary week, which will take place in Moscow in November, issues related to enhancement of measures for technical assistance to member states will be discussed. This agenda is particularly important with regard to more rigid effectiveness requirements in the new FATF Methodology.

Prior to the EAG Plenary session the Eurasian Group delegation will participate in the FATF Plenary meeting, the Presidency of which went to Argentina. Among the agenda's priorities is further development of the FATF standards and assessment methodology, which is especially important for EAG member states before discussion of their own reports.

Another important event of the 2017 fall was the international workshop "Effective Supervision as Mechanism to Ensure Transparency and Stability of the Financial System". The event provided a dialogue between public authorities and the private sector in the Eurasian region and enabled the exchange of best practices of public-private partnerships and organization of AML/CFT supervision. I am sure that such projects allow to gain new knowledge and discuss topical issues.

EAG Chairman
Yury Chikhanchin

III International Workshop "Effective Supervision as Mechanism to Ensure Transparency and Stability of the Financial System"

The event was held on September 20-21 in Moscow. It was addressed to the countries of the Eurasian region and organized by the Russian Federation, which is the Chair of the Eurasian Group on Combating Money Laundering and Financing of Terrorism (EAG), with the organizational support from the International Training and Methodological Centre for Financial Monitoring (ITMCFM) and the State University of Management (SUM).

The workshop welcomed a large audience of more than 150 experts from public and private sector organizations of the EAG member states (Belarus, China, Kazakhstan, Kyrgyzstan, Russia, Tajikistan, and Uzbekistan), and Armenia, which has an observer status in EAG. The event was focused on sharing the supervision experience and best practices in the field of combating money laundering and terrorist financing, and countries preparing for mutual evaluations of their compliance with FATF standards.

"Our meeting will provide, on the one hand, an overview of innovative approaches to supervision practices and communications with the private sector, on the other - feedback from financial institutions on the prospects for improving the effectiveness of compliance procedures", said Galina Bobrysheva, Deputy Director of Rosfinmonitoring.

Vladimir Nechaev, Executive Secretary of the Eurasian Group, underlined that albeit the fact that the next round of mutual evaluations in the EAG had just begun, it was necessary, without wasting time, to implement comprehensive work in countries on the preparation of materials illustrating the effectiveness of work in both the public and private sectors, including collection of statistics, preparation of the most significant cases and examples.

The participants' special attention was attracted by an overview of the main results of mutual evaluations within the framework of the new FATF standards that had already been completed in a number of countries, which was presented by authoritative international assessor Mr. Yehuda Shaffer, Israeli Deputy State Attorney. The expert highlighted that there were many ways to achieve positive evaluation results, and to achieve that goal it was necessary to provide a permanent communication channel, establish contacts and feedback between supervisory, law enforcement agencies, regulatory organizations and the private sector:

"A developed and reliable supervision system for AML/CFT purposes will help to identify and remove violations or omissions in the field of risk management and impose sanctions for such violations. We have a system of sanctions, corrective measures put in place, which force financial institutions to introduce and apply risk assessment processes. In a number of countries, the bodies responsible for supervising the activities of DNFBPs were established. These are minimum requirements that everyone should uphold and apply".

The presentations on the practice of implementing such types of interaction as "Personal Account" and Compliance Council (Russia) attracted a lot of attention. A lively discussion was inspired by the issue on information systems which enable collecting the beneficial ownership information from open sources (China), remote identification and remote opening of bank accounts (Belarus, Russia), new approaches to risk management when implementing Fintech projects (China, Belarus, Russia), as well as typologies for identifying persons with indicators of links to terrorism and drug trafficking (Russia).

The recommendations developed by the workshop participants will be implemented to further advance of national AML systems in the Eurasian countries.

Tools for Effective Risk-Based Supervision

Abstract of the speech by Anjelika Khadanovich (National Bank of the Republic of Belarus) and Svetlana Poddubskaya (Financial Monitoring Department of State Control Committee of Belarus)

The regulatory legal act determining the principles and procedure of control and supervision activity in the Republic of Belarus is the Decree of the President No. 510 dated October 16, 2009. Practice confirmed the effectiveness and feasibility of using risk-based approach for planning inspections, which allows us to carry them out selectively and identify only those entities that have the highest probability of violations of the law. Criteria for the assignment of subjects to the respective risk groups for assignment of scheduled inspections were developed and defined. Their frequency varies from one to five years depending on risk (high, medium or low), which audited entity is marked with.

Coordinating audit plan is formed by the State Control Committee upon the proposals of state bodies for each semester and is in the public domain. For example, in the National Bank the General Directorate of Banking Supervision and General Directorate of Regulation of Non-Credit Financial Institutions make eventual amendments to the plan, given the financial state of banks and companies and questions on the results of remote supervision and control, analysis, reporting, results of previous audits. The decree provides possibility of carrying out unplanned inspections, including on AML/CFT, by decision of the Head of the controlling/supervisory authority.

The National Bank is the mega-regulator which supervises and controls the banking sector and non-credit financial institutions.

In 2010 a risk-based approach in combating money laundering was introduced into the banking system of the Republic of Belarus. When dividing customers into risk groups a three-track model is used. In other words, all the information collected from the clients is grouped into three vectors: risk by the client's profile, risk by geographical region and risk by banking products (i.e. types of financial activities in the bank). As a result of the analysis of each vector with regard to lowering and raising factors work with the client is assigned a total degree of risk – high, medium or low. The process of assigning the final degree of risk to the client is carried out by the matrix.

Since 2015 a risk-based approach in AML/CFT is integrated into non-credit financial organizations as well. It also uses a three-track model of risk distribution, but their scale consists of two degrees – low and high.

An RBA is used by the banks to identify suspicious transactions in activities of customers. Operations by high risk clients are in special focus, their monitoring is carried out daily, and customers with low and medium risk are checked once a month or once a quarter.

Banks do not fill in special forms for the threshold operations, only for suspicious ones. The National Bank formalized forty-five indicators of suspicious transactions. Banks can adjust these characteristics in part of the subject composition of the analyzed period. Out of forty-five suspicious financial transactions` indicators banks can automatically identify twenty-five. Search of automatization algorithms is conducted on nine grounds, automatization of eleven indicators is considered inappropriate (this is the so-called behavioral indicators when the client, for example, behaves inappropriately, acts under somebody's command or under the instructions of a third party, presents documents that cast doubt on the authenticity, etc.).

The basis for detection are algorithms with setting keyword filters, types, number of transactions that are imposed on the accounting system of the bank. The easiest to automate are indictors that contain words identifiable by the context, codes in specific fields of accounting systems (e.g., transactions on loans, payments to certain countries, payment in favor of non-residents to an account in another country etc.). Special forms on suspicious transactions are submitted by banks to the Financial Monitoring Department (FMD) of the State Control Committee of the Republic of Belarus, which has developed its own processes to automate analysis.

The Financial Monitoring Department is a small financial intelligence unit, therefore finding ways of processing, automatic analysis of data sets from different sources is highly relevant. Let's have a closer look at the mechanisms automating the process of analysis of financial transactions subject to special control, or STR. In this regard, it is important to mention technical aspects of introduction of suspicious transactions reports to the FMD. To all reporting entities (financial and non-financial) in Belarus there is a unified format for submitting information. Information is submitted on the transaction, on attempt to commit one, and on transactions during the analyzed period.

An STR consists of three logical parts. Information on each participant is filled in a separate sheet. The data of the payer, the person alienating the property, is always presented in the second part (second sheet), information about the recipient of funds or assets – in the third part (the third sheet). An STR also contains data of the participants, accounts, electronic wallets used in financial transactions, and other information.

The information in the messages is structured in appropriate fields in 8 sections, 14 fields in these sections are filled with values from handbooks, for instance, handbook of financial transactions types, reference suspicion indicators, etc. In FMD there is daily automatic control of incoming electronic (99.6% of all incoming mail) and submitted in hard copy for manual entry STRs. To automatically detect errors algorithms that allow to evaluate an STR at various stages of processing are generated.

Details of the validated STRs are subjected to so-called rapid analysis, when automatic search of SPOs by specified parameters is carried out daily. Such parameters may relate to information about financial transactions or its participants. For example, today in FMD is implemented such daily automatic selection, by various lists, primarily terrorist lists; document numbers of participants used in the financial transaction, and other criteria.

In addition, function of monitoring-control has been automated. It is aimed at notification of received STRs with the STR specified parameter fields defined by the analyst (account number, identification number, etc.). If you match the specified parameters, authorized personnel receive the notification message on mail server for action.

Significant efforts of the FMD are aimed at automatic detection of schemes of receiving and (or) legalization of illicit income. In this regard, the Department has created and is improving a software product that allows to formalize information in STRs, through typologies, maintenance of their list, groups of characteristics that make up the typology.

In such work it is of great importance to create dossiers for different categories of persons (national and foreign, natural and legal) on the basis of incoming data. Each dossier is evaluated. Therefore, the typology is formed on indicators featuring STR participants and the financial transactions mentioned in the provided information. There is a test mode provided for typological schemes formation process, which allows you to create options prior to their approval.

Approved typologies, groups of indicators are assigned with weighted coefficients, which are regarded during update of STR data. For the analyst signs that functioned are visually highlighted. In addition, the reporting in customized forms (templates) is fine-tuned.

Information obtained during automatic pre-analysis further undergoes in-depth analysis with use of analytical tools. If there are indicators of ML/TF information and analytical materials are sent to law enforcement, supervisory and other state authorities. If further analysis doesn't reveal signs of ML/TF, supervision over participants of operations/types of operations continues.

This publication reflects the main approaches to suspicious transactions identification on the stage of implementation and automatization of files received by the FMD in terms of optimal use of resources involved in the national AML/CFT system. Efforts in this area are being constantly aligned.

Risk Management for Financial Innovations

Abstract of the speech by Viktor Dostov, President of the Russian Electronic Money Association (Russia)

We live in a rapidly changing world, encompassing swift changes in financial technology, while old regulatory mechanisms are often too slow to keep up with the vigorous development of the market. Therefore, I would like to speak about a new approach to regulation, namely so-called “regulatory sandboxes”.

Technology is not inherently able to appear in our lives, instead, it comes onto a certain market with existing players, existing regulation, etc. Unfortunately, this market has barriers to the development of such technology, quite numerous barriers, the main of which are regulatory and infrastructural ones. To make sure that all of our innovations develop transparently and openly we need to remove these barriers in an effective and legitimate manner.

What are the principal legal barriers to the emerging and existing financial institutions trying to adopt some efficient technology or other?

First, regulation has always been based on specific business models (card payments, money transfers, corporate payments, etc.). These models provided a basis for all regulatory systems. What comes to us today — bitcoin, crowdfunding, etc. — is different from these models; therefore, this is often too ambiguous for the regulator, which brings these issues to a “grey area”.

Second, modern financial institutions are quite vulnerable. As regards the risk of losing a license, they may prefer to avoid implementing new solutions that are not explicitly permitted under law. This brings about a situation currently known as de-risking. Here, we come to the fact that transparent large organizations that fall under supervision of central banks and financial intelligence are unfortunately not carriers of new technology. Instead, new technology emerges somewhere on the periphery, often beyond the control of the regulator.

Additionally, a similar situation comes from new players. People involved in software solutions for payments and in the creation of algorithms are not always well acquainted with statutory requirements. Traditionally, they are quite difficult; in addition, there are certain justified situations where qualified professionals demand high salaries, there are high costs in general, and there is a great scope of work and software solutions. Often, this is a very serious challenge for startup companies.

When a company enters the market, having, for example, a staff of five, it is really very difficult for the company to afford to implement an appropriate compliance policy or employ a compliance officer. It is also very difficult for such a company to prepare documents and be ready for regulation in the context of potential requirements; it is difficult for such a company to explain to the central bank or tax authorities what it does. Therefore, unfortunately, there are barriers: innovations are expensive and risky, which leads to the risk that traditional financial institutions have advantages in the long run. For them, it is very good; but for consumers, it is bad, because we do not get new technology, service prices remain high, and functionalities remain underdeveloped.

It is clear that all of this is not due to some evil intent of regulators or their desire to support the traditional sector. Regulators have their own problems: it is difficult for them to see innovations in a rapidly growing market. This lack of knowledge leads to the fact that the regulator is not able to adequately assess risks, trying to be on the safe side as always. In addition, there is a significant issue: it is not possible to adapt legislation to each specific innovation.

What approaches are possible here? The first, simple and understandable, is a ban. I will not dwell on this issue, since it is understandable for everyone that a ban can be effective in some cases and completely ineffective in others. There are possibilities of deregulation; I mean, some part of the market is simply taken out of regulation. This is a normal approach; European legislation, for instance, uses a waiver mechanism, whereby small financial companies are relieved of compliance with the e-money directive or the payment directive until the range of their customers or the volume of their monetary transactions becomes sufficiently large. But this approach proved to be not very effective too: if you deregulate one company, this does not impose too much danger. However, if someone starts to massively create small shadow companies beyond regulation, then they constitute, of course, a serious threat to the market.

As I said, it is not possible to adapt regulation to each new technology or business idea. When regulators realized this, they came to the conclusion that, perhaps, special regulatory regimes would work. The “sandbox” is an illustrative example of these regimes. What is it? In plain language, the “sandbox” is a set of rules that allows companies to test their products and business models in real mode without compliance with regulatory requirements subject to the limitations. I would like to clarify this formal definition: “provided that the regulator keeps a close watch on them”.

Something similar applies to “financial sandboxes”. There can be many algorithms, but I will give you the following example for clarity. A company approaches the regulator (the regulator has special staff members for this process) and explains what it does. The regulator establishes the test parameters. For example, the regulator may say, “You have worked for six months, you are able to engage at most a thousand people to provide customer service, and, consequently, you cannot open anonymous purses”. Then, the company periodically reports on the progress in testing. As a result, they jointly prepare some financial report, evaluating the results of these tests. The application includes a description of the work, the need for tests (that is, why this business model does not fit existing legislation), and the results that are planned to be achieved. For instance, they can show financial stability, or that the level of effective compliance in this system is high enough, that is, this business does not allow the use of any mechanisms for money laundering and the financing of terrorism.

It is important to note that this process is quite fast. As exemplified by the United Kingdom, where it is tried and tested to the greatest extent, the period from an application to testing is ten weeks, plus six months from the beginning of testing to the final report. Not only small unlicensed companies but also traditional banks can participate in the process, because they also have a lot of interesting projects, which, to the best of their knowledge, can or cannot fall under existing legislation. And a traditional bank is exposed to a much higher risk of losing its license than a small company.

The regulator can exempt users from some regulatory requirements. Theoretically speaking, if any customer must be physically present at opening an account in Russia, then, in the case of certain players, the regulator can allow, for example, identification by Skype. But no one can tell the bank that now you can identify all users by Skype within six months. Companies periodically report, deadlines are set in the negotiation process, but in any case, this is operational reports for a total of six months.

Now, speaking of how the results are evaluated. First, evaluation is applied to whether the model works. That is, you can offer something that will be useless for anyone, not interesting, and not operational. Second, the appearance of risks is assessed. For example, the opening of Skype accounts is found to result in many dummy accounts. Or in contrast, everything is fine, and the degree of reliability resulting from such automated high-technology tests is much higher than possible errors resulting from verification of identity documents.

The goals and results are quite comprehensible. First, we reduce legal uncertainty and raise the controllability of the innovation process. Second, we increase the availability of investments, because investors in a company understand that they have time to evaluate the result of investment, during which they are, theoretically speaking, free from legal risks. And third, based on all of this, we can create some new rules for future tools and innovative models.

Spanish Presidency of FATF Comes to an End

From June 18 to 23, 2017, Valencia (Spain) hosted the last FATF Plenary meeting under the Spanish Presidency of Mr. Juan Manuel Vega-Serrano. Over 800 representatives from 198 jurisdictions participated in the event

The meeting was opened by Mr. Rafael Catalá, Minister of Justice of Spain, who highlighted the special role of the FATF in countering terrorism financing and money laundering. The Managing Director of the International Monetary Fund, Ms. Christine Lagarde also pointed out the Group's contribution to insuring world's financial and economic security and called on the members of the global network to strengthen joint actions to combat terrorism financing, corruption and tax crimes, and increase transparency of correspondent banking relations.

Mr. Luis de Guindos, Spanish Minister of Economy, Industry and Competitiveness addressed the FATF delegations, emphasizing the top priorities of the Group, including de-risking and beneficial ownership. The key priority of the Spanish Presidency was to build a dialogue with representatives of the FinTech and RegTech sectors.

In accordance with the Operational Plan, the Group is implementing a number of measures aimed at counter-terrorist financing (CFT). The delegates decided to launch a number of projects in the future to identify the TF sources, methods and channels. The Plenary recommended information sharing among all member states, which would facilitate the procedures for requests of terrorist-linked funds or other assets freezing. The meeting adopted the report on inter-agency information exchange, targeting both traditional participants of the CFT system and organizations commonly not involved in this activity. The document sets forth best practices and practical tools for improving collaboration and information sharing within jurisdictions concerned.

The meeting discussed the progress of a report on information sharing with the private sector (aimed, among other things, at identifying the terrorist financing activities), and continuation of research into recruitment financing for terrorist purposes.

Delegates also discussed current outcomes of the joint FATF-Egmont Group research project on vulnerabilities linked to beneficial ownership. Among a number of issues, this project determines the mechanisms used to conceal the beneficial ownership of legal entities. The FATF joint expert meeting with banks' representatives held in Moscow (Russia) contributed to the project fostering.

De-risking has been among top priorities of the FATF since 2014. To date, significant work has been done in this area, namely, a guide for risk-oriented approach, including money and value transfer services. The FATF will consider the use of guidance by national competent authorities and the financial sector. The delegates discussed the recent de-risking developments and updates, including access of the money transfer sector to the banking services. To solve this problem, the FATF closely cooperates with the Financial Stability Board, the IMF and other organizations.

The Plenary adopted a revision to the Interpretive Note to Recommendation 7. Its text was aligned to comply with the recent resolution of the UN Security Council. The revised version clarifies the use of targeted financial sanctions and is aimed to disrupt financing of proliferation of weapons of mass destruction.

In 2016, the FATF commenced an interim review of its current mandate to analyse the opportunities for further strengthening the capacity and effectiveness of the global network. The FATF members discussed proposals to achieve these goals. The discussions resulted in an agreement to extend the President's term and strengthen the role of the Vice President. These reforms will enter into force after a three-year transition period.

FATF heads of FIUs met with representatives of several international banks and had productive discussions on how to enhance the effectiveness of suspicious transaction reporting regimes, as well as on recent measures to foster development of public-private partnerships. The Forum approved a paper on identification of areas where further work would increase the effectiveness of international AML/CFT efforts.

Argentina Heads FATF

Since 1 June 2017 the FATF President is Mr. Santiago Otamendi, the Secretary of Justice of the National Ministry of Justice and Human Rights of the Republic of Argentina

For a long time the country was in the FATF "grey" list, but it managed to overcome the existing problems and demonstrated significant progress of the national AML/CFT system.

As the main goal for his Presidency, Mr. Otamendi has identified countering financing of terrorism. It is the direction in the Hamburg Declaration endorsed by the G20 leadership. Also the focus is on assessment of the national AML / CFT systems effectiveness during the fourth round of mutual evaluations, and on increase of financial flows transparency, beneficial ownership issues etc.

Another top priority for the FATF President is building up relations between the FATF and judicial authorities. In his opinion, this channel is still ill-tuned, which brings additional difficulties and risks to the global financial security. Mr. Otamendi since 1987 has been working in various institutions of the Argentina's judicial system, including as criminal judge. In his practice he faced problems that can pop-up in the course of international standards integration into national legislation. In his view, the Argentine's scope both as the FATF President and as a country is to provide judges with a more aligned legal system for timely response to relevant ML/TF risks.

Mr. Otamendi considers it necessary to adopt at national level the law on corporate responsibility for combating corruption and determining beneficial owners of legal entities. Due to recent significant inflow of foreign funds to the national economy this issue is becoming one of the most relevant for Argentina.

***

Ms. Jennifer Fowler, the Deputy Assistant Secretary for Terrorist Financing and Financial Crimes at the U.S. Department of Treasury was appointed Vice-President by the FATF Plenary meeting. For a long time she headed the national delegation to the FATF, participated in the development of the first-ever guidance on combating weapons of mass destruction proliferation financing. Also Ms. Fowler is the Co-Chair of the FATF International Cooperation Review Working Group, and before that cochaired Policy Development Working Group.

We welcome you to take part in the development of the EAG Bulletin. If you would like to place news, articles and other publications in the following issues of the Bulletin, please feel free to send an e-mail entitled "EAG Bulletin" to: info@eurasiangroup.org

Telephone: +7 (495) 950-31-46, fax: +7 (495) 950-35-32.
More information can be found on our website:
http://www.eurasiangroup.org

Publisher: Autonomous Non-Profit Organization ITMCFM.
Editorial board: P. Kukushkin, I. Lisina.