Belarus – the main stages in developing a national AML/CFT system

The Republic of Belarus attaches great importance to activities in combating money laundering and financing of terrorism. Belarus is constantly improving its national legislation in this field, and basing its work on expert evaluations and FATF standards.

The formation of the national AML/CFT system in Belarus started in 2000 with the approval of a framework law on combating money laundering.

In 2003, the Financial Monitoring Department of the State Control Committee of the Republic of Belarus was created as a national financial intelligence unit (FIU). The department consists of three offices – analytics, coordination and international cooperation, and that of information and technology. The chief of the department is Valery Yaroshevsky.

Within a year after creating its own FIU, Belarus took part in the Founding Conference of the Eurasian group on combating money laundering and financing of terrorism and became one of the founding member states of EAG. To a large extent, the active stance of Belarus as an EAG member state is determined by the fact that the chief of its national FIU has occupied the position of EAG Deputy Chairman since 2008. In 2008, the Republic underwent EAG mutual evaluation. The results of the evaluation pointed out the fact that the country continues its work in trying to achieve harmonization of its national legislation and the elimination of shortcomings revealed in the course of the mutual evaluation. It has also improved measures for client identification and determination of beneficiaries of financial transactions, introduced requirements for the monitoring of foreign political and economic entities and international organizations.

Belarus pursues active work within the EAG, while also participating in the work of other international organizations in the field of AML/CFT. For instance, since 2007 the financial intelligence unit of Belarus has been a member of Egmont Group.

This group unites financial intelligence units from all over the world. In November 2009, Belarus, Russia and Kazakhstan created a Customs Union, within the framework of which a separate agreement on AML/CFT is being prepared. Belarus also took the lead in founding the Council of CIS Heads of FIUs, and in November there was a meeting held in Minsk to consider a draft Agreement for the foundation of this organization.

Chronicle of events
- September 2003 – a national FIU, the Financial Monitoring Department of the State Control Committee of Belarus, was created by decision of the Belarusian President.
- October 2004 – at the founding Conference in Moscow, Belarus became a member of the EAG.
- May 2007 – the Egmont Group accepted the Financial Monitoring Department of the State Control Committee of Belarus as a full member of its organization.
- December 2008 – the EAG peer evaluation of Belarus was completed.

Russian President

Valery Yaroshevsky: “We are steadily on the road to full compliance with international standards”

EAG Deputy Chairman, Director of the Financial Monitoring Department of the State Control Committee of the Republic of Belarus speaks about the progress of the national legislation in the field of AML/CFT and shares his views on the prospects of expanding international cooperation.

Recently, FATF-style regional bodies started paying more and more attention to money laundering and financing of terrorism risks in the field of electronic payments. What countermeasures to these very high-priority risks are now being applied in Belarus?

It is true that the question of electronic money and its use for money laundering is still very close and is widely discussed by regional groups and the expert community. In Belarus, and in fact in all CIS states, the supervision of electronic money is receiving very close attention. A number of corresponding measures have been approved. In accordance with the national legislation, only credit institutions may act as emitters of electronic money, and the registration of such institutions is performed by the National Bank. Transactions involving electronic money are subject to tighter monitoring measures. Overall, we can say that Belarus has quite well-developed legislation in the field in question, and the country continues in developing new statutory regulations.

As to the legislation, we know that recently Belarus has approved a package of enactments for an improved national AML/CFT system. What innovations are included here?

This past year, many new enactments as well as amendments to laws already in effect have been introduced. For instance, the framework law on AML/CFT received the definition of a “beneficiary owner” and introduced a special definition for foreign politically-exposed persons. It also introduced criminal and administrative responsibility for individuals and legal entities for the illegal use or disclosure of information contained in the register of security holders. There is also responsibility specified for illegal use or disclosure of information on the results of financing and operating activities of the issuers.

Thus, Belarus has criminalized insider trading and market manipulation.

Overall, these changes are aimed at the further harmonization of national laws, and these bring Belarus closer to full realization of international standards.

In early November, Minsk hosted the second meeting of the expert group on refinement and coordination of the founding document for a new international organization, the Council of CIS Heads of Financial Intelligence Units. Belarus was one of the first states to support the idea of its creation. Please tell us, what inspired this interest in the creation of such a structure in our region?

The Council’s activity will be aimed at developing the legal base for cooperation in the field of AML/CFT throughout the Commonwealth of Independent States. We will be able to substantially strengthen integration among countries that are participating in the regional system of combating criminal money laundering and financing of terrorism. In fact, this is another format for cooperation, which is performed at somewhat a different level than that of EAG cooperation, namely at the level of FIU heads of those countries who are members of two regional groups for combating the financing of terrorism – the Eurasian Group and MONEYVAL.

What would be the benefit of this? In the first place, expanded exchange of information at the stages of its collection, preliminary investigation, court proceedings, execution of judgment and creation of a single database in the field of AML/CFT. In the second place, the opportunity for coordination of joint activities for the revelation and suppression of money laundering schemes.
This event brought together representatives of financial intelligence units, law enforcement and supervisory bodies, IT and finance specialists and the providers of electronic payment services. The varied group of participants was able, to a large extent, to determine the complex nature of the discussion, which focused on electronic money and risks of its use for criminal money laundering and financing of terrorism. Typology studies in these topics have been made by EAG and MONEYVAL experts. With every passing year, Internet banking technologies are progressing while more and more users from all over the world are starting to participate in the circulation of electronic money. However, the criminals are keeping up with this progress as well, and for them the global network has become a true goldmine – hacking, embezzlement and shady virtual transactions are now made quickly and anonymously, with minimal risks and maximum profits. At the same time, the counteraction to cybercrime is considerably hindered by a number of factors, which can only be overcome through the joint efforts of financial intelligence, supervisory bodies and the private sector. This is the opinion with which all international experts, taking part in the seminar, agreed. For instance, in his address, EAG Chairman, Oleg Markov placed special emphasis on the fact that the problem of countering criminal flows on the Internet acquires a peculiar urgency with the progress of electronic technologies and requires consolidating efforts of the entire global community.

MONEYVAL Chairman, Vladmir Nechayev referred to the role played by the EAG/MONEYVAL joint seminar in this process. “The experts, speaking at this seminar, have clearly demonstrated how widely the criminal element can use the newest electronic technologies and requires consolidating efforts of the entire global community.”

Experts also recommend the introduction of threshold amounts for electronic transactions, requirements to refuse performance of electronic payments without their destination being specified, special requirements for the provision of information on payment details and submission of transaction data to FIUs, licensing the activities of the electronic money systems, etc.

Alexander Seger, who led one of the topical sections of the seminar, offered a principal division of cyber crime into two kinds – crimes of the “computer vs. computer” type (stealing identification and other data, seizing control over a system) and crimes committed by way of a computer (hacking bank accounts with the purpose of further plunder of their funds, etc.).

He also drew the attention of participants to schemes that criminals are using to launder money.

“Cyber swindlers also leave some tracks and we should be able to “read” them and suppress criminal schemes. This activity receives great contributions from the FATF and regional FATF-style regional bodies such as EAG and MONEYVAL, as they study relevant typologies and distribute best practices to financial intelligence units, law enforcement and supervisory bodies as well as to the private sector. They do this within the framework of similar seminars, conferences and consultations as this.”

According to Mr. Kaspersky’s estimates, the annual damage to the world economy from cyber criminals has exceeded the $100 billion figure. A particular threat to the society is presented by cases when computer malware infects systems that control industrial objects. Taking into account the trans-border nature of cybercrime, it should be combated both at the national and global levels by uniling the efforts of governments, specialized agencies and international organizations, and this is where Mr. Kaspersky agrees with AML/CFT experts.

Within the framework of the second section of the seminar conducted by Co-Chairs of the EAG Working Group on Typologies, Igor Volovyevich (Federal Financial Monitoring Service, Russia) and Alexei Feschenko (State Agency for Financial Monitoring, Ukraine), the risks of using non-banking financial institutions, alternative payment systems and foreign trade operations for money laundering were discussed. Participants of this seminar section specified the main trends and criminal schemes, and provided recommendations for reducing ML/TF risks in the above-mentioned sectors.

Results of the seminar will be recorded in summarized typology reports on the risks involved in using electronic money for AML/CFT purposes, and on criminal financial flows on the Internet, which EAG and MONEYVAL experts will bring up for discussion by the Plenary Sessions in December.

In the follow-up to the plenary session, materials on the typology studies will be published, according to Yuri Chikhanchin, head of the Federal Financial Monitoring Service, who closed the seminar. “We have learned to recognize the tracks left when economic crimes are committed,” he emphasized. “Cyber swindlers also leave some tracks and we should be able to “read” them and suppress criminal schemes. This activity receives great contributions from the FATF and regional FATF-style regional bodies such as EAG and MONEYVAL, as they study relevant typologies and distribute best practices to financial intelligence units, law enforcement and supervisory bodies as well as to the private sector. They do this within the framework of similar seminars, conferences and consultations as this.”
Electronic money – threat or reality?

E-commerce is rapidly developing, but the criminal world is no less active in trying to take advantage of the technological benefits provided by the Internet in the field of electronic payments. International experts and representatives of national AML/CFT systems of the Eurasian region speak on threats and joint measures for combating cybercrime.

Electronic technologies in the financial field – the historical background

A little more than fifty years ago, the Bank of America issued the first universal debit card called Visa. Nine years later its competitor, MasterCard, appeared. The new products facilitated the development of information technologies in the banking sector.

In 1975, the first cash machine was placed into operation in the USA, and the first point-of-sale terminal appeared in another four years. In such a way, began the development of electronic payments. The first chip card for small purchases emerged just 15 years ago, almost at the same time when the first electronic wallet in the world was invented.

Within a year, members of the international e-commerce system started to think about developing information security principles. That is how rules for conducting electronic transactions appeared, in particular the SET protocol, though these were not widely applied.

Back in 2000, there were about a hundred payment systems operating in the world. Nowadays there are several hundreds of these, available in 37 countries of the world. The most well-known systems are PayPal, E-Gold, and StormPay; in Russia – WebMoney, YandexMoney, Cyberplate and some others.

Criminal financial flows on the Internet

The scopes of cybercrime are increasing every year. Yevgeniy Kaspersky, the head of Kaspersky Laboratories, the largest in the world Russian IT security company, believes that the level of cybercrime will only grow. “More and more services are now going online, and so is the money. And where there is much money, there are also many people trying to steal it.”

Electronic money is often used by drug traffickers. Having received their stock, retail drug dealers transfer available funds into the “electronic wallet” of their wholesaler from the nearest instant payment terminal and simultaneously send an SMS informing him about the made payment. As a result, the initial stage of criminal money laundering is complete.

Another example was taken from the experience of Russian law enforcement agencies. As a result of clampdown on terrorist and extremist organizations, the following scheme was discovered and liquidated. A criminal group registered a number of fictitious noncommercial organizations engaging in social activities. All accounts were managed by way of Internet banking technologies. Non-cash monetary funds from commercial enterprises arrived into the accounts of these organizations as donations and contributions. Afterwards these funds were transferred to the debit cards of fictitious individuals, and then the participants of the scheme withdrew the money. A part of these funds was used to finance extremist activities.

Reality of the law

Cyber banditry is a relatively new kind of criminal activity, the effective counteracting of which requires the formation of a corresponding legal framework.

Experts of the Eurasian Group on combating money laundering and financing of terrorism note that the regional countries are engaged in active work on developing legislation in the field of Internet payments.

In Belarus, they achieved considerable results in the field. The country’s electronic payments market is regulated by two special resolutions issued by the Board of the National Bank of the Republic of Belarus, approved in 2001 and 2003.

In Uzbekistan, electronic money settlements are regulated quite well, as the law “On Electronic Payments” was adopted five years ago.

Legal regulation of electronic money circulation in Kyrgyzstan is performed according to the law “On the payment system of the Kyrgyz Republic.”

In Turkmenistan, the “Provision on Electronic Payments” approved by the President’s Decree on February 2000, is currently in effect.

A draft law introducing the notion of “electronic money” and regulating a number of questions concerning their emission, circulation and redemption in Kazakhstan was developed in the summer of 2009. Experts believe it may be approved in 2010.

China also has some interesting experiences to offer. In the summer of 2009, the national government approved a decision to prohibit the use of electronic payment systems for the purchase of real goods. Now one can only buy virtual presents and pay for virtual entertainment with electronic money.

In Russia, the Ministry of Finance of the Russian Federation with the participation of the Federal Financial Monitoring Service conducts active work in development of legislation regulating electronic technologies in the financial sector. The Ministry of Finance of the Russian Federation with the participation of the Federal Financial Monitoring Service, the Central bank and other agencies prepared a draft federal law “On the National Payment System” in order to ensure legal regulation of payments and settlements with the use of electronic money.

In the opinion of Pavel Livadny, the Co-Chair of the EAG Working Group on Mutual Evaluations and Legal Issues and chief of the Legal Department of the Federal Financial Monitoring Service, approval of a real law should create the basis for legal groundwork of the electronic payments market and substantially increase the effectiveness of the national AML/CFT system.

International experts are united in the opinion that the risks of using electronic money for criminal purposes continues to grow, and the need for rapid development of information technologies.

Forming unified approaches to the regulation of payments and other technologies in the financial sector is becoming an important priority of the international community. A large role in solving these problems is given to the FATF and FSRBs, which analyze all relevant trends and formulate recommendations for reducing ML/TF risks for private sector institutions.

FATF Plenary Session in Paris

One of the main points on the agenda of the Plenary Session, which took place in late October in France, was the continued work on preparing a new edition of 40+9 FATF Recommendations – being the AML/CFT world standards.

Review of the Recommendations is aimed at creating an improved effectiveness of the global system in conditions of new threats and emerging risks and is determined by the aspiration of the international community to unify approaches to countering economic crimes, corruption, terrorism, etc.

The amendments discussed provide for an extended field of application of the risk-based approach, inclusion of tax crimes into the body of those predacious of money laundering, refined requirements for monitoring of transactions using electronic technologies, as well as for the proliferation of enhanced due diligence to be applied towards financial activities of national PEPs (in addition to foreign officials).

Improving the recommendations is, to a large extent, aimed at realization of the initiative on the application of financial monitoring mechanisms for countering corruption. This topic is one of higher priorities of FATF under the Presidency of Mexico. Participants of the plenary session have noted that an important role in reviewing standards is assigned to private sector institutions, which can actually evaluate various aspects of their practical application. To study the entire range of financial community opinions in the most accurate way, FATF will hold a series of consultations with the private sector.

The first consultative forum took place in Paris in late November 2010. FATF has also continued its work on studying the situation in high-risk and non-cooperative countries.

In its public statement, the FATF draws attention to Iran and Democratic People’s Republic of Korea, which are in the ML/FT high-risk zone and pose a threat to the world financial system. As for Teheran, FATF calls for the adoption of countermeasures. The second public document, representing the results of the on-going monitoring of the international standard compliance review, draws attention to a group of states, where the national AML/CFT systems have serious deficiencies, though considerable work is being done to eliminate these, including high-level commitment. Azerbaijan and Qatar achieved positive results in improving anti-money laundering regimes and were therefore excluded from FATF enhanced monitoring within the framework of this procedure.

The plenary session approved the FATF typologies reports on money laundering through new payment methods and ML risks involving trust companies.
Recent events

European Parliament to remove obstacles to effective development of the international e-commerce market

Representatives of the European Parliament announced the need to create a united e-commerce market for the European community.

Experts estimate that the revenues from this kind of trade will reach 100 million EUR within two years. This past May, the European Commission started using a new digital program, which is going to bring noticeable improvements to the quality of electronic transactions, according to the developers of the system. By 2012, all e-commerce websites, guaranteeing the quality and reliability of their services, will receive a corresponding certification label.

Russia-Tajikistan: Strengthening co-operation

Within the framework of further development of bilateral cooperation between the countries, the Prime Minister of the Russian Federation visited Tajikistan.

The Russian delegation, headed by Prime Minister Vladimir Putin, held a series of meetings with Tajik authorities. Issues of cooperation in the field of economy, security and joint countering of the terrorist threat and drug trafficking were discussed at the top level.

The head of the Federal Financial Monitoring Service, Yuri Chikhanchin, visited Tajikistan as a member of the delegation. With his partners from Tajikistan, he discussed development of the national AML/CFT regime compliance with international standards and recommendations on its enhancement.

Tajikistan and Turkmenistan joined the EAG in 2010. Previously it held an observer status within the organization.

Russian banks may refuse clients

Amendments to the law that regulates combating criminal money laundering have been introduced to the State Duma of the Russian Federation. New recommendations affect the control of all cash transactions exceeding the sum of 600,000 rubles.

Banks will acquire the right to refuse performing suspicious transactions for clients on the grounds of submitting false documents to open an account or attempting transactions lacking evident economic substance.

In accordance with the amendments introduced, the only exclusion can be made for inter-bank transactions and transactions between banks and the Central Bank, as these are connected to ensuring their operating activities, which is encryption from correspondent accounts at the Central Bank and cash servicing of their clients.

The authority of the UN should be used in the global struggle against money laundering

On the initiative of Russia, a meeting involving security agency representatives from 43 countries took place in Sochi on October 5-6, 2010.

This meeting was also attended by Security Council secretaries, national security assistants and UN representatives.

In his speech, chief of the Russian Security Council, Nikolay Patrushev, noted that combating money laundering is an actual problem for most countries. Laundering criminal money involves companies working on a legal basis, such as banks, non-banking financial institutions and gambling establishments, and this fact hinders the work of competent authorities all over the world.

Participants of the meeting believe that development of a universal convention, within the UN framework, may facilitate the effectiveness of combating money laundering at the global level.

Results of the “Kanal-2010” operation summarized

The Kanal-2010 operation, which involved officers from anti-drug, law enforcement and frontier guard agencies from the CSTO member states, as well as financial intelligence units from EAG member states, was held on November 16-22.

Seven agencies from almost 25 countries of the world, including China, the USA, Italy, Iran and Turkey, joined the operation as observers.

As a result of operational procedures, there have been confiscated 6.6 tons of drugs, more than 40 tons of precursors, over 1,000 weapons and 17,000 rounds of ammunition. More than 4,000 people received criminal charges, with 267 of these being members of criminal groups. The operation put an end to many channels of synthetic drug trafficking from Europe and cocaine smuggling lines from Latin America in the water zones of the Black and Caspian Seas.

The Coordination Council, unifying the heads of competent anti-drug trafficking authorities in CSTO member states, highlighted the effectiveness of financial intelligence units within the framework of the Kanal-2010 operation, as FIUs submitted information, to law enforcement agencies, for further inspection of 32 legal entities.

Dushanbe. Seminar on combating drug trafficking

At the Agency for Drug Control (ADC) of Tajikistan in Dushanbe, a training session for law enforcement agency officers was held.

The EAG is creating an interactive expert community in order to discuss the current issues and share experience with the aim of bringing together specialists in the field of financial monitoring, financial security, law, banking technologies and others engaged in global AML/CFT processes.

The opportunities created by the EAG portal allow experts to hold interactive forums, carry out research and discuss the current AML/CFT initiatives.

We welcome all experts that wish to join us in this work to fill in a form at www.eurasiangroup.org (follow the “Expert Community” link).