

**Eurasian Group on Combating Money Laundering and
Financing of Terrorism**

(EAG)

WORKING GROUP ON TYPOLOGIES (WGTyp)

**Organized criminal groups (including those formed along ethnic
lines) in operations (transactions) with cash and non-cash assets**

Contents

Introduction	2
1. Organized Crime Concept. International and National Legislation	3
2. Activities of Organized Crime Groups and Fight against them in the Surveyed Countries	6
3. Specificities of Activities of Organized Crime Groups Involved in Cash and Cashless Transactions	12
4. Specificities of Maintaining by FIU of Information on Organized Crime Groups, Organized Criminal Associations, their Members and Activities	23
Conclusion	24
Annex No.1. Indictment: The United States of America against Mariana Feliksova Lozanova accused of online auction fraud (<i>see WGTYP (2011) 10 Annex 1</i>)	
Annex No.2. Indictment: The United States of America against Bernard Rommel and others accused of Ponzi scheme fraud (<i>see WGTYP (2011) 10 Annex 2</i>)	

Introduction

Pursuant to the decision of the 11th Plenary Meeting of the EAG member-states held in December 2009 the Federal Financial Monitoring Service of the Russian Federation and the Financial Intelligence Service of the Kyrgyz Republic steered the typology exercise: Cash and Cashless Transactions Involving Organized Crime Groups Including Ethnic Crime Groups.

The topic of this typology exercise was proposed by the representative of the Financial Intelligence Unit of Kyrgyzstan at the meeting of the Working Group on Typologies (hereinafter WGTYP) and was endorsed by other parties participated in the meeting.

This typology exercise is focused on studying various aspects of the fight, with involvement of the financial intelligence units, against the organized crime activities.

The main objectives of this typology exercise are:

- Identify specificities of activities of organized crime groups, including ethnic criminal groups, related to cash and cashless transactions;
- Compare the experience gained by the financial intelligence units of the EAG-member and observer states in course of their engagement in the fight against organized crime and develop recommendations for enhancing efficiency of these efforts.

In course of the research the questionnaire drafted jointly by the Financial Intelligence Units of Russian and Kyrgyzstan was distributed among all EAG-member states and EAG observers.

The Financial Intelligence Units of the following countries took part in this survey:

- The Republic of Belarus;

- The Kyrgyz Republic;
- The Russian Federation;
- The Republic of Armenia;
- The Republic of Tajikistan;
- The Republic of Uzbekistan;
- The Italian Republic;
- The United States of America.

The information and materials supplied by the parties participated in the survey vary in terms of completeness. The most detailed responses to the questionnaire with the description of a number of investigations of activities of the organized crime groups were provided by the United States of America. Besides that, the detailed information on the research topic and the investigation examples provided by Russia and Kyrgyzstan were also included in this Report.

In general, the available materials allow for making important comparative assessment of the efforts undertaken by the surveyed countries to combat organized crime activities.

Today, organized crime (including transnational crime) is reasonably considered one of the global problems and challenges of our time. With wide variety of unlawful activities, and particularly unlawful economic activities, it is the operation of the organized crime groups that poses the most serious and increasing threat to the social and economic security as well as to the political stability of the countries. This growing threat requires undertaking vigorous joint efforts to eliminate criminal networks, deter traditional and new types of criminal offences and combat laundering of criminal proceeds. In this context, all developed countries pay exceptional attention to combating organized crime, to improvement of their national legislation and to deterring activities of criminal groups.

1. Organized Crime Concept. International and National Legislation

Since the organized crime is the extremely complex phenomenon there are many different approaches to formalizing its components in the regulatory and conceptual definitions. Such wide range of definitions is explained by the fact that no single definition can cover the entire variety of types of organized crime since it is featured by economic, regional and ethnic differences among organized crime groups.

In this context, the definitions formulated by the international organizations are of special importance. The basic international document for combating the organized crime is the United Nations Convention against Transnational Organized Crime adopted on November 15, 2000 by the Resolution of the 62nd Plenary Meeting of the 55th Session of the General Assembly of the United Nations Organization. By now, 156 United Nations (UN) member states have acceded to the said Convention.

This Convention does not contain a general definition of “organized crime”. Instead, the Convention uses the operational approach under which this complex phenomenon is defined through description of its individual components. The Convention defines the following concepts that are the essential components of organized crime:

a) “Organized Criminal Group” means a structured group of three or more persons, existing for a period of time and acting in concert with the aim of committing one or more serious crimes or offences established in accordance with this Convention, in order to obtain, directly or indirectly, a financial or other material benefit;

b) “Serious Crime” means conducts constituting an offence punishable by a maximum deprivation of liberty of at least four years or a more serious penalty;

c) “Structured Group” means a group that is not randomly formed for the immediate commission of an offence and that does not need to have formally

defined roles for its members, continuity of its membership or a developed structure.

The national legislation of the surveyed countries also includes legal provisions that are aimed at combating organized crime and define, to greater or lesser extent, the concept of organized crime and its features.

For example, although the Racketeer Influenced and Corrupt Organizations Act (commonly referred to as the RICO Act) currently in force in the United States does not contain the “organized crime” concept, this Act has been originally aimed at fighting against its criminal practices and manifestations. The US Department of Justice has adopted the comprehensive definition of the international organized crime, however, this definition has not been included in the said Act.

In Italy, the concept of gangster association (mafia) is provided in the Penal Code, and there are also a number of laws and regulations called the anti-mafia legislation.

The Republic of Belarus has adopted the Law on Combating Organized Crime and defined the “organized criminal group” in the Criminal Code.

In the Republic of Armenia, the “organized crime” concept is not used in the criminal legislation, however, the Criminal Code defines the types of complicity in crime, one of the forms of which are offences committed by organized group and offences committed by criminal association.

Similar provisions are contained in the Criminal Code of the Republic of Uzbekistan which defines the organized criminal group and criminal association concepts through the description of forms of complicity in criminal offences.

The Criminal Code of the Republic of Tajikistan gives more detailed definition of the organized criminal group and criminal association concepts. In addition to the Article that defines the types of accomplices in crime, the Criminal Code contains the separate Article that covers criminal offences committed by a group of persons by previous concert or by an organized group or by a criminal

association, and also includes the Article that imposes criminal liability for creating a criminal association.

The Criminal Code of the Russian Federation also contains the provision that imposes liability for commission of criminal offences by an organized group or by criminal association (criminal organization) as well as liability for establishment (organization) of a criminal association (criminal organization) or membership in such association (organization).

The legislation of all countries that took part in the survey indicates common attributes of organized crime. These attributes include the organized nature, stability, cohesion and strict control, and besides that, the purpose of establishment and operation of organized crime groups is the commission of offences for gaining material benefits.

At the same time, from our viewpoint, the attributes of organized crime are most completely specified in the legislation of the United States of America and Italy. In addition to the aforementioned features, the US Department of Justice has identified the following attributes that define the organized crime concept: committing violence or other acts of intimidation; exploiting differences between countries for pursuing their objectives; gaining influence in government, politics and commerce; obtaining economic gain not only from patently illegal activities but also from investment in legitimate businesses; and insulating both their leadership and membership from detection, sanction and prosecution.

The Italian Penal Code provides the following concept: “The illegal association is of mafia type when the participants take advantage of the intimidating power of the association and of the resulting conditions of submission and silence (omerta), to commit criminal offences, to manage or control, either directly or indirectly, economic activities, concessions, authorizations, public contracts and services, and to obtain other unlawful profits or advantages for themselves or for others”.

2. Activities of Organized Crime Groups and Fight against them in the Surveyed Countries

The law enforcement system of each of the surveyed countries includes the independent agencies, or units incorporated in the law enforcement agencies, that specialize in combating organized crime. The responses provided by the countries that took part in the survey revealed two major ways of establishing and operating the national anti-organized crime systems. For example, Italy and Armenia have independent units empowered to fight against organized crime (the Anti-Mafia Investigation Department and the National Anti-Mafia Directorate in Italy and the General Directorate for Combating Organized Crime in Armenia). In the United States, the necessary powers are vested in a number of law enforcement agencies within the scope of their respective authority, while the general coordination of these efforts is assigned to the Attorney General's Organized Crime Council. In the Russian Federation, the anti-organized crime functions also fall within the scope of authority of various law enforcement agencies.

Information on the government agencies engaged in combating organized crime in all surveyed countries is presented in Table 1.

Table 1. Government Agencies Engaged in Combating Organized Crime

Country	Name of the Government Agency
USA	The US Attorney General's Organized Crime Council, the Organized Crime and Racketeering Section within the Criminal Division of the Department of Justice, the Federal Bureau of Investigation, the Drug Enforcement Administration and other.
Russia	The General Prosecutor's Office of the Russian Federation, the Investigation Committee of the Russian Federation, the Ministry of Internal Affairs of Russia, the Federal Security Service of Russia, the Federal Drug Control Service of Russia, the Federal

	Migration Service of Russia – within the scope of powers vested in them
Italy	The Anti-Mafia Investigation Department (Department of Police), the National Anti-Mafia Directorate (Prosecutor's Office)
Belarus	The special anti-organized crime units within the Internal Affairs Agencies, the National Security Agencies and the General Prosecutor's Office
Armenia	The General Directorate for Combating Organized Crime within the Police of the Republic of Armenia, the Unit against Human Trafficking, Drug Trafficking and Organized Crime within the General Investigation Department
Kyrgyzstan	The Ministry of Internal Affairs, the National Security Agencies, the Customs, the State Service on Drug Control - within the scope of powers vested in them
Tajikistan	The Ministry of Internal Affairs in coordination with the Prosecution Agencies, the National Security Service and the Customs Authorities
Uzbekistan	Department for Combating Organized Crime within the Ministry of Internal Affairs

The criminal activities of the organized groups are not limited by commission of just ordinary crimes (such as murder, theft, extortion, etc.). In parallel, they are actively engaged in commission of economic crimes and are developing new types of crimes including those involving the use of new technologies, such as environmental crimes, cyber crimes, financial fraud and theft of intellectual property. Listed below are the main types of criminal offences committed by the organized crime groups.

- Gambling,
- Bookmaking,

- Theft,
- Illicit drug trafficking,
- Labor racketeering,
- Usury,
- Fraud (inter alia, in the financial and credit sector, and creating Ponzi (pyramid) schemes),
- Human trafficking,
- Migrant smuggling,
- Illicit arms trafficking,
- Smuggling,
- Prostitution,
- Extortion,
- Corporate raiding,
- Tax evasion,
- Money laundering.

Presented in Table 2 are the criminal offences most frequently committed by the organized crime groups and criminal associations in the surveyed countries.

Table 2. Areas of Organized Crime Activities

Country	Most Common Criminal Offences Committed with Involvement of Organized Crime Groups					
	Smuggling, Counterfeiting of Products	Illicit Arms and Drug Trafficking	Fraud	Money Laundering	Cyber Crime	Theft
USA	✓	✓	✓	✓	✓	✓
Russia	✓	✓	✓	✓	✓	✓
Italy	-	-	✓	✓	✓	✓
Belarus	-	-	-	-	-	✓

Armenia	-	-	-	-	-	✓
Kyrgyzstan	-	✓	✓	✓	-	✓
Tajikistan	✓	✓	✓	-	-	✓
Uzbekistan	✓	✓	-	-	-	-

The above Table clearly shows that organized crime groups operate in all countries. At the same time, the financial intelligence units of the United States, Russia and Tajikistan have the information on operation of international organized crime groups, while the information on operation of ethnic organized crime groups is available only to the FIUs of the United States and Russia.

For example, operating in the United States is the Italian-American organized criminal society (La Cosa Nostra) as well as the Eurasian, Albanian and other Balkan, Asian, West-African and Middle-Eastern organized crime groups. And according to the available information operating in Russia are the Asian and African organized crime groups as well as the ethnic organized crime groups consisting of the immigrants from the Former Soviet Union Republics.

We can use the Russian Federation statistics to assess the percentage of criminal offences committed by the organized crime groups in total number of committed crimes.

According to the Russian Federation Ministry of Internal Affairs the ratio of criminal offences committed by the organized crime groups to total number of the committed crimes (the main types of criminal offences are considered) is as follows:

Table 3. Number of Solved Crimes and Crimes Committed by Organized Crime Groups and Organized Criminal Associations, which are Subject to Mandatory Pretrial Investigation (as of the end of 2009)

Type of Criminal Offences	Solved	Committed	% of Solved
---------------------------	--------	-----------	-------------

		by Organized Crime Groups and Associations	Criminal Offences
Total	838027	31397	3.75
Murder and Attempted Murder	15373	183	1.19
Grievous Bodily Injury	35275	42	0.12
Kidnapping	418	64	15.31
Theft	293244	2902	0.99
Fraud	72723	10253	14.10
Robbery	45736	294	0.64
Armed Robbery	21270	643	3.02
Extortion	3859	433	11.22
Banditry	168	168	100,0
Creation of Criminal Association	212	212	100,0
IT Crimes	11296	30	0,27

The above data show that the greatest number of criminal offences committed by the organized crime groups involved fraud – a total of over 10 thousand of fraud-related crimes, or 14.1% of their total number, were solved by the law enforcement agencies in 2009. The practical work conducted by Rosfinmonitoring and the Russian law enforcement agencies shows that the organized crime groups commit complex large-scale frauds such as creation of Ponzi (pyramid) schemes, fraud in the financial and credit sector, etc.

Besides that, financial investigations of the criminal offences committed by the organized crime groups (criminal associations) is more labor and time consuming compared to other financial investigations.

Thus, in course of their practical work the financial intelligence units need to know and take into account the specificities of activities carried out by the organized crime groups and the typologies indicators of the criminal offences typically committed by organized crime groups.

3. Specificities of Activities of Organized Crime Groups Involved in Cash and Cashless Transactions

As mentioned above, the main purpose of establishing a criminal association is to obtain material benefits through commission of criminal offences. It is obvious that the professional criminal activities generate huge amounts of “dirty” money and the fight against laundering of this money is the main mission of the financial intelligence units.

At the same time, it is important to note that the financial intelligence units have sufficient capabilities for detecting not just the indicators of laundering of criminal proceeds but also the indicators of predicate offences. This also applies to criminal offences committed by organized crime groups and organized criminal associations.

The surveyed countries provided a number of typologies of predicate offences and the follow-on laundering of criminal proceeds committed primarily by the organized crime groups and the related examples of financial investigations of such crimes. It is also noteworthy that the financial intelligence units are capable of proactively detecting suspicious activities that match these typologies.

Typologies and Financial Investigations: Case Studies

A) Money Laundering through Fictitious Bank Accounts (information provided by the Italian FIU)

This is the wide-spread method which is based on “obedience” and/or negligence of financial intermediaries. Criminal groups typically operate the actual network of straw men for withdrawing cash against cheques and also for making

payments by cash obtained from illegal activities. And such networks operate under the supervision of apparently well-known and respectable professionals (the so-called ‘white collars’) who are not members of the organization to avoid any suspicions.

One of the types of the straw man schemes is the so-called phishing – Internet fraud committed by hackers engaged in theft of personal data. Such hackers use servers located abroad and send e-mails to online banking customers for stealing passwords, obtaining access to personal accounts and transferring funds in illegal manner. The specificity of phishing is that bank accounts of natural persons are used without their consent.

In such situation, a modern network of straw men consists of the so-called “financial managers” hired by criminal groups on the Internet. Their task is to receive large amounts of funds on their bank accounts, withdraw cash and transfer this cash through remittance companies in favor of certain individuals abroad, whose details they receive by the SMS messages or via the online message transmission system. For their services such “financial managers” charge between 5 and 10 percent of the amount of the funds transferred.

Besides that, of particular interest is the so-called “**Nigerian**” fraud scheme which involves the use of accounts of natural persons opened under fictitious names (*information provided by the Russian FIU*).

Most frequently this type of fraud is committed by the organized crime groups consisting primarily of the Nigerian nationals. The scheme used by them is as follows: Copies of the websites of large Russian or foreign companies are created in the Internet. After that, lucrative commercial proposals are sent on behalf of such companies to various foreign companies. Then the criminals start e-mail or telephone negotiations with those who responded to the proposal for convincing a potential victim to transfer money to the account of the company which name is misused by the fraudsters. In doing so, instead of providing the

bank details of the company fraudsters often give to a potential victim the details of a straw man, whose name in Latin is similar to the company's name. As soon as funds are transferred to such account the criminals withdraw cash or transfer these funds abroad to other members of the criminal group for their laundering.

For example, for committing the fraud with the use of the fake website of Baltic Main Oil Pipelines company (the company's short name is Baltnefteprovod) the fraudsters opened the bank account using the false passport issued in the name of BALT NEFTEP ROVOD.

Thus, the key indicator of this typology is one off transfer of funds by a company located abroad to an account of a natural person who is the citizen of Nigeria or other African country with the follow-on cashing out the received funds. And the name of such natural person should be similar to the name of a large national or foreign company.

It is important to note that it is difficult, for obvious reasons, to detect and identify fraudsters who use false passports. At the same time, one should take into account the fact that the same fraudster may use several passports in different names for opening accounts in various banks. However, such passports will have the photo pictures of one person. Thus, potential frauds with engagement of various parties may be linked together by the involvement of the same real person.

B) Money Laundering through Bank Loans (*information provided by the Italian FIU*)

Workers who receive low wages apply for a loan, which amount is too high for them to repay. In doing so, they use fake or overestimated copies of salary certificates and tax returns as well as guarantees issued by their employers.

Local banks accept the prepared documents and a criminal group receives back its illicit proceeds through legal repayment of bank loans.

The similar scheme has been developed to use guarantees issued to businessmen by foreign banks for laundering illicit proceeds. In particular, large

amounts of money obtained as a result of misappropriation/theft of funds and/or tax evasion committed by businessmen are deposited in foreign banks. After that, these businessmen apply to other banks for loans and credit lines, which repayment is secured by the guarantees issued by the foreign banks.

Thus, this scheme allows a businessman to:

- Reuse the “laundered” money;
- Be granted tax exemption from taxable interest rate and additional expenses related to funding the Italian banks.

And finally, there is a similar scheme with involvement of legal entities – the so-called three-party financial transactions with the countries that have offshore zones for depositing illegal funds abroad. These schemes are used in some cases related to money laundering and tax evasion in the situations when the national “concealment” systems appear to be less safe and more vulnerable.

This simple method is based on the following mechanism:

- Shell companies located in the countries with tax heaven issue invoices in order to justify transfer of “dirty” funds and to reuse them anonymously in the international financial markets;
- Other companies make payments under non-existing transactions.

C) Fraud and Money Laundering through Ponzi Schemes (information provided by the Russian FIU)

Various types of Ponzi (pyramid) schemes are widely used in many countries all over the world, including the Russian Federation. Such schemes are quite often created by organized crime groups.

In three recent years, Rosfinmonitoring conducted over thirty successful financial investigations of operation of such fraudulent investment schemes. Quite often Ponzi schemes are run on a large-scale basis covering several regions of the country, and tens of thousands of people may become their victims. The results of

criminal investigations of such crimes often capture the headlines and are socially important.

The experience gained in course of the conducted investigations allowed for identifying the following distinctive features and indicators of Ponzi schemes:

- Promising, in advertisements and promotional materials, to pay the guaranteed interest on invested funds at a rate higher than the average market rate along with declaration of minimum risk;
- Promising to invest attracted funds into new highly-profitable projects and businesses;
- Concealing the information on the company's top manager and owners and the official details of the company;
- Company is not the member of the self-regulatory organizations operating in the financial market;
- Recruiting agents whose remuneration depends on amount of attracted funds;
- Posting advertizing materials mainly in free advertisement newspapers and on web-sites;
- Attracting funds under loan agreements (the most typical method);
- Using the online payment and postal transfer systems for receiving funds transferred for the investment projects;
- Accumulating by a company of funds received from a large number of natural persons and using a significant portion of the received money in shadow transactions and transferring them in favor of senior managers and owners of such company.

The task of the Rosfinmonitoring's analysts is to detect such indicators as soon as possible in order to convince the law enforcement agencies to start checking the received intelligence before the claims of the first victims are received. Some financial investigations achieved this objective. For example,

Rosfinmonitoring has detected the fraud indicators at the early stage of operation of North Investment Siberia pyramid scheme and informed the law enforcement agencies thereof. At that time, the streets of one of the Russian cities were full with the billboards of the company that created the said fraudulent investment scheme, and no claims of the first victims had been received yet. Nevertheless, the law enforcement agencies launched the inquiries and, in the end, the individual who had created that scheme was found guilty by the court of committing the large-scale fraud with involvement of the criminal group and was sentenced for seven years of imprisonment.

Another example of the successful large-scale financial investigation is connected with the operation of Garant Credit pyramid scheme, which during a short period of time opened dozens of its offices in Russia, Ukraine and Belarus. Over 350 thousand people became victims of Garant Credit Ponzi scheme and the incurred financial losses amounted to 18 billion rubles. Despite extremely complex and multi-layered nature of this fraudulent financial scheme the conducted financial investigation revealed indicators of laundering of the funds received from the investors. In particular, information on transactions involving acquisition of a number of real estate was filed with the law enforcement agencies.

The example of investigation of **CYTX** Corporation Ponzi scheme provides more detailed information on involvement of organized crime groups in creation and operation of pyramid schemes (*information provided by the US FIU, Annex 1*).

D) Money Laundering through Shadow Financial Service Schemes
(*information provided by the Russian FIU*)

One of the priorities of financial analysis conducted by Rosfonvonitoring is to detect large-scale shadow financial service schemes in order to provide information support to the law enforcement agencies in deterring operation of such schemes, identifying persons who create them and revealing money laundering

indicators in the activities of creators of such schemes. Operation of such schemes is of especially dangerous nature since they are designed for supporting large flows of funds that have criminal origin or are intended for certain criminal purposes. Criminal proceedings against persons involved in this type of illegal activity have been most frequently instituted under Article 172 of the RF Criminal Code, i.e. this criminal offence has been defined as illegal banking operations. It is also important to note that when funds of various customers “flow” through the shadow financial service schemes they get mixed, which makes the analysis of operations carried out by such customers extremely difficult since in most cases it is impossible to identify funds when they “flow out” of such schemes. Therefore, the investigators face obvious difficulties in identifying the ultimate recipient of such funds, determining illegal proceeds and detecting money laundering indicators.

In recent years Rosfinmonitoring conducted over one hundred of successful financial investigations of operation of the shadow financial service schemes. The experience gained in course of these investigations show that quite often the provision of the shadow financial services has been arranged by the organized crime groups including owners, senior managers and employees of banks. It is important to note that in most cases financial investigations and provision of information and materials to the law enforcement agencies resulted in deterrence of operation of the detected schemes. Besides that, the banking licenses of over thirty credit institutions have been revoked based of the results of these financial investigations. However, since investigation of illegal banking operations is extremely complex and requires large-scale efforts, the law enforcement agencies not always managed to successfully complete investigations and turn the matter over to the court.

The high-profile case is the financial investigation of the operations of Sodbusinessbank that ran the shadow financial service scheme through which “dirty” money has been flown.

Rosfinmonitoring launched financial investigation of the operations of this bank in 2003 after the famous crime was committed – kidnapping and murder of the top managers of KamAZ-Metallurgy company. According to the investigators this crime was committed exclusively for (receiving) ransom. The criminals demanded that the ransom in amount of 1 million US dollars had to be transferred to the shell company's accounts opened with Sodbusinessbank. The financial investigation, that was initially launched for tracking the flow of money transferred to three customers of Sodbusinessbank as the ransom for the kidnapped persons, revealed the large-scale shadow financial service scheme, which resulted in arrest of a number of the bank managers. The funds from Sodbusinessbank accounts were withdrawn as the unsecured loans amounting to 2.5 billion rubles provided to the companies which characteristics indicated their fictitious nature. Three senior managers of the said credit institution were accused of involvement in this crime, one of whom admitted his guilt and is currently convicted and sentenced to imprisonment.

Besides that, in December 2007, the Arbitration Court of Moscow Region passed the decision on holding the former managers of the bank subsidiarily liable for the obligations of the bank and on recovering 1.42 billion rubles from them. It is the record-high amount that has been recovered by the arbitration court decisions. Thus, in the end the creators of the said shadow financial scheme incurred both criminal and financial liability.

It is noteworthy that the aforementioned financial investigation made it possible to reveal the structure and the roles of the parties engaged in the large-scale shadow financial service scheme, and the detailed description of the scheme provides a range of attributes and indicators that enable analysts to detect similar schemes.

This shadow financial service scheme was well structured and consisted of several levels of accounts opened by fly-by-night companies and accounts opened in the names of straw men.

The first level consisted of several dozens of companies that collected funds intended for various purposes and received from a large number of actual shadow financial service customers and transferred those funds to the second level.

Operating at the second level were several fly-by-night companies that further accumulated and mixed funds intended for various purposes by transferring all received money to another fly-by-night company that operated at the third level. The latter company accumulated all shadow money flow. At the fourth level the money flow was split into several flows for the intended purposes: funds to be transferred abroad, funds to be cashed-out, funds to be used for acquisition of assets in the stock market. The funds were cashed out by several dozens of straw men, and were transferred abroad through couple of fully controlled offshore companies. A portion of funds transferred to the accounts of the aforementioned offshore companies was cashed out in foreign currency through the bank accounts of the non-resident straw men.

Thus, the structure of the shadow financial service scheme is intended for mixing funds transferred by a large number of customers for various purposes at the first stage and splitting them for the indented purposes at the second stage. And the parties that are engaged in such schemes and perform these operations have two distinct financial profiles. The first profile is typical for a company with fictitious characteristics which has much more counterparties to the credit transactions than to the debit transactions, while the second profile features the inverse ratio. Therefore, the analysis of statistical data on the number of counterparties of parties to transactions makes it possible to detect, accurately enough, companies featured by the aforementioned financial profiles and, based on this, to reveal shadow financial services schemes.

E) Theft of Credit Institution's Assets and Laundering them through Fictitious Securities Acquisition Agreements (information provided by the Russian FIU)

Organized crime groups commit not only traditional offences of a clearly criminal nature (extortion, arms, drug and human trafficking, etc.) by also actively infiltrate into the financial and credit sector and select banks (their liquid assets) as their victims, which results in a credit institution bankruptcy.

One of the examples of such illegal activity of organized crime groups is the financial investigation conducted by Rosfinmonitoring in connection with the fraud involving withdrawal of liquid assets of the credit institution through the fictitious securities acquisition agreements.

The mechanism of the designed criminal scheme is as follows:

Members of the organized crime group had some money, which they used for the acquisition of a small credit institution that performed actual banking operations and had depositors and other customers (Alpha bank).

After that, the shell investment company licensed to perform brokerage and depository operations and fully controlled by the leader of the organized crime group (Beta company) became the customer of Alpha bank. Then, Alpha bank entered into the agreement with Beta Company to acquire a package of liquid securities of a large securities issuer, and pursuant to this Agreement transferred all available funds, including those of its depositors, to the investment company's account. The latter issued to the bank the extract from the depository certifying deposition of the securities into the custody account as envisaged by the agreement. But in reality, the investment company did not acquire any securities in favor of the bank and the extract from the depository was the false one. Thus, funds, including the customers' funds, were withdrawn from the bank.

Beta company transferred all funds received from the bank to the accounts of the members of the organized crime group as loans or as the repayment of their

own funds under the brokerage agreements. It is noteworthy that the amount of funds withdrawn from the bank and eventually received by the members of the organized crime group was significantly higher than the amount of funds spent by them for the acquisition of the bank. This balance constituted the criminal proceeds which were further invested for the acquisition of another bank.

After that, theft of the Alpha bank's assets resulted in its bankruptcy. In this situation losses were incurred by the depositors and other customers of the bank and also by the Government, since it compensated, through the Federal Deposit Insurance Agency, a portion of funds lost by the bank's depositors.

This scheme is of especially dangerous nature since it is easily replicated by fraudsters. The investigation conducted by Rosfinmonitoring revealed the fact that the same organized crime group had used the described scheme to acquire and bankrupt several credit institutions. And each next bank acquired by that group was larger than the previous one.

The most distinct indicator of this typology is the transactions carried out by Beta company. Such Company carried out small number of transactions and had small number of customers. It received large amount of funds from one or several credit institutions against securities. But in practice it carried out no securities acquisition transactions and transferred the received funds as loans or under the brokerage agreements to natural persons or to other fictitious or offshore companies.

I) *Criminal Cases (information provided by USA)*

In the framework of this typology study, the US has provided the examples of the criminal cases investigated in connection with the activities of the organized crime groups related to the online auction fraud (Annex 1) and running the Ponzi scheme (Annex 2).

Although this information is not directly related to the activities and operations of the financial intelligence units, it contains a lot of details

characterizing various aspects of criminal offences committed by the organized crime groups and reflects the logic of the conducted judicial investigation that made it possible to prove the guilt of the accused persons. Therefore, this information is of certain value for the FIU analysts.

4. Specificities of Maintaining by FIU of Information on Organized Crime Groups, Organized Criminal Associations, their Members and Activities

The questionnaire distributed among the surveyed countries did not include questions related to arrangement of recording and maintaining by the FIUs of information on organized criminal associations, their members and activities. At the same time, in course of this typology exercises it became obvious that proper maintenance of such information is extremely important for enhancing efficiency of the efforts undertaken by the FIUs to combat organized crime. This conclusion follows from the simple logical reasoning:

The financial intelligence units, by filing requests or otherwise, receive information from the law enforcement agencies on organized criminal associations (organized crime groups), their activities, structure, leaders and members as well as on the companies and institutions controlled by them. And such information is provided mainly in form text files. To effectively use this information it has to be properly structured and entered into the FIU's information system in form of the relevant objects and links between them. And the entity that describes an organized criminal association (organized crime group) should be the key object, while other objects (leaders, members, controlled companies, etc.) should have the relationship/links with it.

The issue pertaining to the arrangements for maintaining information on organized crime was discussed at the meetings of the EAG Working Group on Typologies in course of discussion of the interim results of this typology exercise.

The discussion revealed that the FIUs of the EAG-member states did not use the aforementioned approach.

It seems that the financial intelligence units have significant potential in this area for enhancing the effectiveness of their efforts aimed at combating organized crime.

Conclusion

Organized crime constantly strives to spread the areas of its influence, infiltrate in various economic sectors and to extend its influence on the executive, legislative and judicial authorities. Therefore, the fight against organized crime is one of the priorities of many law enforcement agencies in various countries.

Various criminal offences committed by organized crime are evidenced in financial transactions and deals which often have distinctive features. In some cases in order to commit offences and launder the obtained criminal proceeds the organized crime groups, along with the cash settlements, also use the financial and credit mechanisms, which allows the financial intelligence units to proactively detect involvement of organized crime groups in illegal activities (inter alia, at the early stages) and to inform the law enforcement agencies on such facts. These indicators enable the financial intelligence units to proactively detect suspicious activities that may be related to the operations carried out by organized crime groups.

Thus, it seems that the financial intelligence units are able to enhance the efficiency of their involvement in combating organized crime through the development and use of typologies of suspicious activities typical for organized crime. In doing so, the proper information exchange should be arranged with the law enforcement agencies and between the FIUs.

Another potential enhancement of the effectiveness of the efforts undertaken in this area involves maintenance of information on organized crime

groups (organized criminal associations) at the level of objects and links between them in the FIU's information system.