ЕВРАЗИЙСКАЯ ГРУППА
по противодействию легализации преступных доходов
и финансированию терроризма

EURASIAN GROUP
on combating money laundering
and financing of terrorism

WGTYP (2012) 10

28 - December - 2012
English – Or. Russian

For Official Use

17th EAG PLENARY MEETING

November 5 – 9, 2012

India, New-Delhi

MONEY LAUNDERING AND TERRORIST FINANCING WITH USE OF PHYSICAL CASH AND BEARER INSTRUMENTS

For any inquiries, please, contact the EAG Secretariat:

Dmitry PUTYATIN, Tel.:+ 7 495 607 16 62, E-mail: Putyatin@eurasiangroup.org

Please bring this document with you to the meeting as no paper copies will be available at that time

Table of Contents

Introduction

As part of the Eurasian Group 2012 Action Plan, approved at the EAG 15th Plenary meeting, the Republic of Belarus has conducted an international study titled "Money Laundering and Terrorist Financing Involving the Use of Cash and Monetary Instruments".

The goals of this study are:

- define the indicators of money laundering and terrorist financing offences involving the use of cash and monetary instruments;

- identify vulnerabilities in the activities of banks and non-bank financial institutions (remittance service providers) requiring special attention because of the risk of money laundering transactions, and define their indicators;

- draft the guidelines for the application of measures designed to reduce or eliminate such risk.

The need for a research on this topic was supported by all working group participants.

As part of the study activities, Belarus drafted and distributed among the member and observer countries a special questionnaire.

The study was conducted using the responses contained in the questionnaires completed by the following countries:

- Russian Federation;

- Ukraine;

- Republic of Turkey;

- Republic of Serbia;

- Kyrgyz Republic;

- Republic of Uzbekistan;

- Republic of Armenia;

- Republic of Kazakhstan.

Alongside the information obtained from member and observer countries, the study also contains data provided by the Belorussian competent authorities.

General Provisions

A stable state and steady development of the monetary sector, coupled with a proper management of the national system of monetary circulation, is the key condition for sustained economic growth. Cash is an essential element of monetary circulation and its status in a great variety of cash transactions remains unchanged, unlike the status of non-cash funds that take the form of bank account records.

As the pace of digitalization speeds up, the idea that cash will gradually disappear giving way to digital money becomes increasing popular. However, it's important to remember that the current potential of cash even in developed countries is far from being exhausted. For example, cash transactions account for 75% of all retail transactions in the U.S.; 76-86% in Europe and 90% in Japan. The prevalence of cash is largely due to a rather later advent of electronic means of payment. To date, cash is used to maintain the flow of goods and services, as well as to pay pensions, benefits and insurance claims.

According to the data obtained in the course of the study, a majority of respondent countries have lately been recording an increase in the volume of cash in their economies. A growth in the demand for cash in the economy triggered by the rising national output, price increases or other reasons results in the need for a corresponding increase in the money supply by banks. However, it should be noted that any increase in the volume of cash in the economy also increases the risk of its use for criminal purposes.

Among the key factors encouraging the use of cash are:

- the availability of financial instruments, such as bills of exchange, traveler's checks, bearer shares, bank checks, etc, that allow payments to be made in cash;

- the existence of the shadow economy;

- low level of non-cash payments among individuals paying for goods and services;

- population's informal income, which is derived and stored in the form of cash.

A growing use of cash in settlement transactions and business results in such negative consequences as:

- lower budget revenues caused by the shrinking tax base;

- a shift in the money supply balance in favor of cash, which greatly complicates the planning and management of the economy and, as a consequence, undermines economic stability and social well-being of the state;

- contributes to the growth of the shadow economy and development of the gray market, given that the monitoring of cash flows is much more difficult;

- increases the risk of creation of illegal "centers" for extremist and terrorist financing activities, which in turn, pose a threat to public safety.

In view of the threats associated with cash circulation, it's essential for countries to pursue a consistent and tough policy in the area of AML/CFT and to regularly update national legislation governing the circulation of cash and monetary instruments by tapping into the AML/CFT-related experience of the relevant international and supranational organizations.

Based on the analysis of data obtained from the countries that participated in the study, we can conclude that Russia, Belarus, Uzbekistan, Ukraine, Armenia, Kyrgyzstan, Kazakhstan, Turkey and Serbia have all adopted the appropriate laws governing the circulation of cash and monetary instruments.

Among the measures designed to prevent money laundering and terrorist financing that have been developed and used at the state level are:

- mechanisms for identifying clients, both legal entities and individuals, who carry out cash transactions. The identification mechanism for individuals involves obtaining the following information: name, surname, patronymic, ID document details (passport details for residents and non-residents; residence permit and migration card details for stateless persons and refugees), place of residence or place of stay. The identification mechanism for legal entities involves obtaining the following information: company name and its legal status (OJSC, CJSC, LLC, PE, etc.), taxpayer identification number, place of state registration and the actual location;

- criteria for suspicious transactions and thresholds used to evaluate financial transactions in terms of AML/CFT.

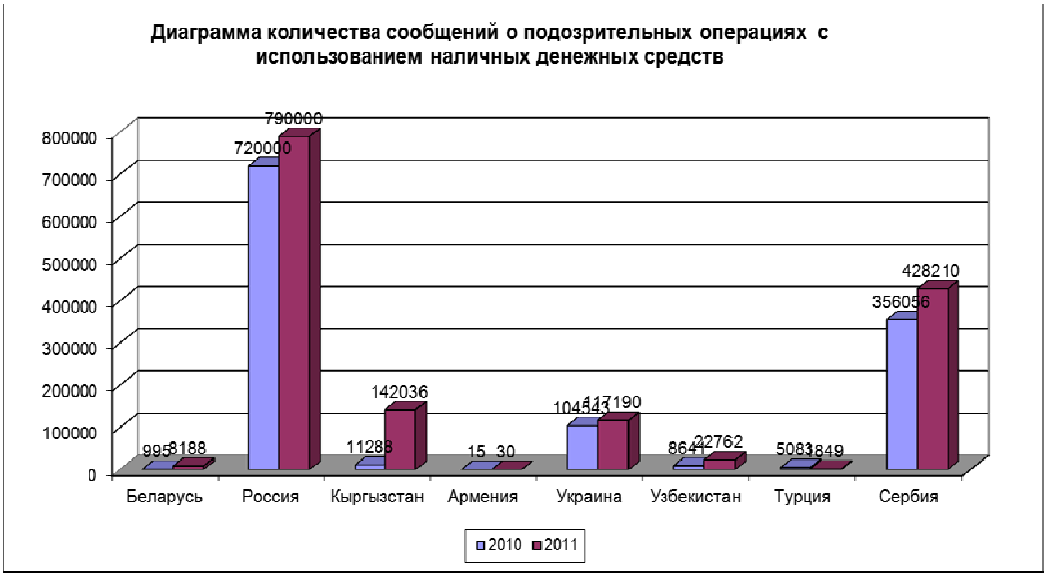
The responsibility for the implementation of AML /CFT measures with regard to client identification and reporting suspicious transactions rests with the persons carrying out financial transactions (banks and non-bank financial institutions engaged in the provision of remittance services, such as Western Union, electronic payment systems, etc.); with regard to the adoption of proactive AML/CFT measures, with the competent authorities and, above all, with the FIU.

The information obtained from the countries participating in the study indicates that the number of reports about suspicious cash transactions submitted to the FIU in 2011 increased significantly compared with 2010. So, for example, 22,762 out of a total of 33,431 suspicious transaction reports submitted to the FIU of Uzbekistan in 2011 related to cash transactions (these figures for 2010 were 8641 and 17,151 respectively). Growth in the number of suspicious transaction reports involving cash was also recorded in Russia (790,000 reports in 2011 against 720,000 in 2010), Ukraine (117,190 reports in 2011 against 104,543 in 2010), Kyrgyzstan (142,036 reports in 2011 against 11,288 reports in 2010), Armenia (30 reports in 2011 against 15 in 2010) and Belarus (8188 reports in 2011 against 995 reports in 2010).

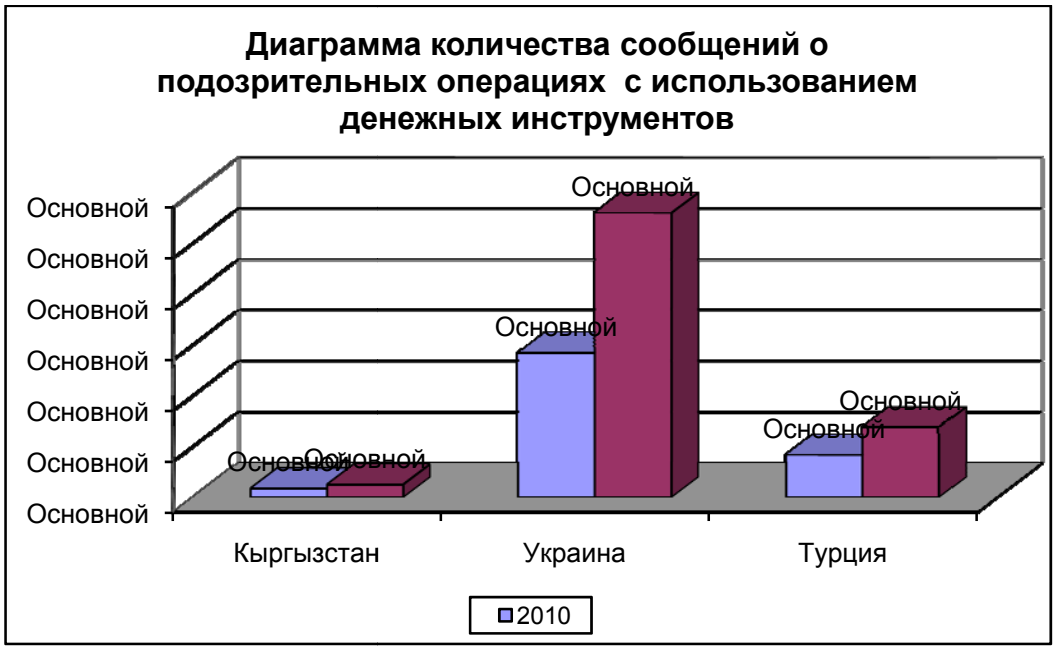
At the same time, it should be noted that the use of cash for unlawful activities is more common than the use of monetary instruments. This may be due to the fact that, on the one hand, the circulation of monetary instruments (bills, bearer shares, traveler's checks, bank checks, etc.) is severely restricted, or outlawed altogether (issue of bearer securities is prohibited in Uzbekistan), while on the other hand, the use of monetary instruments has never become very popular for various reasons (specifics of the economic model, the state of the economy, the level of economic literacy, etc.) among the residents of countries of the former Soviet Union. But this does not mean that in the future the use of monetary instruments will not be as popular as the use of cash.

Below are the comparison graphs showing how many reports about suspicious transactions involving cash and monetary instruments were submitted to the FIUs of respondent countries.

Suspicious transaction reports involving cash (Belarus, Russia, Kyrgyzstan, Armenia, Ukraine, Uzbekistan, Turkey, Serbia)



Suspicious transaction reports involving monetary instruments (Kyrgyzstan, Ukraine, Turkey)



As for the most popular cash-out methods, the study has revealed the following statistics:

Typical cash-out methods

Remittance systems (Western Union, etc.) 22%

Payment systems (PayNet, WebMoney, etc.) 11%

Cashier's desk in banks, ATM; 67%

Cases related to money laundering and terrorist financing with use of physical cash and bearer instruments

Based on the operating experience feedback provided by Belarus, Russia and Ukraine, we can give a few examples of the use of cash and monetary instruments in illegal activities and highlight indicators of such suspicious transactions.

The most common cash-out methods used in Belarus are:

- regular withdrawal by individual entrepreneurs of funds from their bank accounts as personal income through bank cashier's desk;

- transfer of funds by individual entrepreneurs to their personal card accounts and their subsequent withdrawal through ATMs;

- regular withdrawal by legal entities of funds through bank cashier's desk for economic needs;

The examples provided by Belarus were identified in the course of audit measures conducted by the Belorussian law enforcement agencies on the initiative and with the information support of the Financial Monitoring Department of the State Control Committee of the Republic of Belarus.

For example, while reviewing suspicious transaction reports submitted by one Belarusian bank concerning several entrepreneurs who made regular large withdrawals of incoming revenue, the Financial Monitoring Department indentified a group of business entities whose activities exhibited indirect indicators of pseudo entrepreneurship (a mismatch between the financial transactions that are being carried out and the stated activity, low tax burden, execution of transactions that make no obvious economic sense). Following a comprehensive review, all the data related to the activities of these entities were referred to law enforcement authorities.

The investigative work conducted in response to the information provided by the Department has revealed evidence of pseudo entrepreneurial activities carried out by a criminal group, which used the details, bank accounts and seals belonging to four individual entrepreneurs and one legal entity to run the following scheme:

Funds were deposited to an account of one fly-by-night company by several business entities operating in the real sector of the economy as payment for different goods (building materials, radio parts, food, office supplies). Within a few hours of their arrival, the credited amounts were then transferred in their entirety to the accounts of 4 individual entrepreneurs, who, in turn, converted the money into cash by concluding bogus commission contracts with companies located in the neighboring states from which they allegedly received goods later sold to Belorussian companies. The cash was then used to purchase foreign currency, which, according to the company's documents, was allegedly transferred to the companies in the neighboring countries. In reality, however, the foreign currency in cash was transferred to the businesses against the fund transfers made to the accounts of individual entrepreneurs, net of fees paid to the criminal group. The illegal activities of the criminal group generated revenue of 3.6 billion BYR, which is equivalent to $423,529 at the official rate of the National Bank of Belarus.

A total of 18 criminal cases were initiated under Article 233 "Illegal business activities", 234 "Pseudo-entrepreneurship" and 243 "Evasion of taxes and duties" of the Criminal Code of the Republic of Belarus against the members of the criminal group and their counterparties.

Thus, by using the services of illegitimate businesses, Belarusian companies managed to legalize goods purchased by them from grey-market sources and entered in the books using fake invoices provided by illegitimate businesses. It should also be noted that in addition to legalizing grey-market goods, these business entities also evaded taxes, given that the price of goods written in fake invoices is much higher than the actual price paid for the grey-market goods. Therefore, by increasing the expenditure side, the criminals reduced the tax base.

Typical indicators of suspicious cash-out schemes involving the use of individual entrepreneurs' bank accounts are as follows:

1. Depositing funds into the accounts of a fly-by-night company and individual entrepreneurs as payment for dissimilar goods (food, building materials, clothing, computer accessories, auto parts, advisory services).

2. All, or almost all (up to 97%), of the funds deposited into the accounts of individual entrepreneurs are cashed out as personal income, or ostensibly for business needs, almost immediately after being credited (withdrawal period varies from 15 minutes to several hours).

3. Low tax payments (0.01% - 0.97%, and less frequently 1% - 3% of revenue) or complete absence thereof.

4. The post of the founder, manager or accountant of a front company that accumulates funds and transfers them to the controllable individual entrepreneurs is, in most cases, occupied by a person from socially disadvantaged backgrounds (a person of no fixed abode, with drug or alcohol addiction, or a former convict).

5. The company is not located at its registered address.

Example 2.

While studying suspicious transaction reports submitted by banks, officials came across a business entity that was transferring large amounts into card accounts of individuals as payment for used tools, equipment, scrap metal and loans. A further analysis revealed another 3 entities engaging in the identical activity. The funds credited to the accounts of these individuals were subsequently withdrawn in full through ATMs. An in-depth analysis of the available to the Department data on the identified entities responsible for making these transfers and individuals who received them has revealed the following:

- the activities of the identified entities display characteristics of illegitimacy: the payment purpose of the transfers made to the accounts of the suspicious firms read "for computer equipment", "for pallets", "for building materials" and "for car parts". All expenditures made by the suspects were related to transfers of funds to the card accounts of individuals, with "for used uniforms", "for used equipment", "for metal scrap", "for loans" stated as payment purpose. No tax payments were made;

- posts of founders and senior managers were occupied by individuals with a criminal record;

- natural persons whose card accounts were credited were from disadvantaged backgrounds (people with drug and alcohol addiction, with no fixed abode), unemployed, and not listed as employees of these businesses.

A key feature of this scheme is that funds were cashed out by natural persons and not by individual entrepreneurs.

Example 3.

While using intelligence provided by the Financial Monitoring Department, police investigated the activities of I. Ivanov, P. Petrov and S.Sidorov, residents of one Belarusian town and members of a criminal group who, while acting on behalf of and using the banking details, headed paper, accounting documents, seals and bank accounts of the controllable individual entrepreneurs and legal entities established to cover up illegal activities, carried out on the territory of Belarus illegitimate currency conversion and cash-out transactions. For this purpose, they converted funds in Belarusian rubles credited to the accounts of the said controllable businesses into U.S. dollars, Russian rubles and euro, prior to cashing them out. The amount of revenue obtained through the use of this criminal scheme was valued at 24.9 billion Br. rubles.

A set of measures designed to hide the shady business and minimize the risk of disclosure of criminal activity developed by I. Ivanov jointly with P. Petrov and S. Sidorov included measures to create the appearance of legality of the businesses whose accounts were used for illegal financial transactions, i.e. their state registration, registration with tax authorities, appointment of directors and registration as individual entrepreneurs of the controllable individuals who were not aware of the criminal nature of the business. In addition, the secrecy system used by the criminals involved the use of forged primary accounting documents designed to create the appearance of legality of the illegitimate business engaged in by the controllable entities, including through the use of accounting forms; opening accounts, both in Belarusian rubles and in foreign currency, for use in illegal financial transactions; the simultaneous use of multiple accounts belonging to the controllable individual entrepreneurs for the purpose of splitting large amounts; minimizing the end-of-the-business-day cash balance on accounts of the controllable entities; submission of tax reports; regular replacement of entities whose accounts were used in the illegal business; use of figurehead directors and nominal entrepreneurs, who were given instructions as to their behavior, in their communication with regulatory and law enforcement bodies.

By performing the responsibilities they jointly assigned to themselves, I. Ivanov and P. Petrov legally registered two business entities (T and B) in town O, individual entrepreneurs K. Kovalev, A. Kondratov, S. Popko, A Kozlov, P. Pimenov, and S. Sidorov, as well as purchased the documents of the already registered but actually defunct entrepreneurs V. Vashko, N. Izotov and L. Migulev.

With the goal of generating illegal income, I. Ivanov jointly with P. Petrov and S. Sidorov opened accounts for the above-mentioned bogus businesses in several of the country's banks and signed service contracts for the use of the automated cashless payment system Client-Bank, which allows users to make remote payments, send and receive documents, including account statements, and receive authorizations to use the funds on accounts belonging to the controllable entities.

After creating conditions for conducting illegal business, gaining remote access to the bank accounts of the controllable entities, and acquiring the right, through the use of authorizations, to manage funds placed on the accounts of the said entities, I. Ivanov jointly with P. Petrov began to establish contacts with entities seeking to legalize goods purchased with cash from grey-market sources or to convert non-cash Belorussian rubles into foreign currency in cash.

The next stage in the implementation of the criminal scheme involved the conversion of non-cash Belarusian rubles deposited into the accounts of the bogus entities B and T and

individual entrepreneurs K. Kovalev, A. Kondratov, S. Popko, A Kozlov, P. Pimenov and S. Sidorov into foreign currency in cash (U.S. dollars, Russian rubles and euro).

In order to forge the accounting documents, signatures and seals of the controllable bogus entities that were needed to the create the appearance of legitimate business, to cover up the illegal financial transactions carried out by the group participants and to conceal the very existence of the illegal business, I. Ivanov jointly with P. Petrov hired skilled accountant, as well as used the services of individual entrepreneurs K. Kovalev, A. Kondratov, S. Popko, A Kozlov and P. Pimenov, who were unaware of the criminal nature of the business.

After receiving electronic requests from their clients containing the information necessary to produce fake supporting documentation, I. Ivanov jointly with P. Petrov forwarded them to A. Kozhemyako, who prepared fake primary accounting documents subsequently validated with the seals of entities they controlled.

The forged sales, supply and commission contracts and supporting documentation, which were used as the basis for the transfer of funds to the accounts of the bogus entities, were then presented by I. Ivanov and P. Petrov to their clients for signing and stamping with the counterparty seals, and made part of accounting records of the bogus entities. Once the non-cash Belarusian rubles have been received, they were converted into foreign currency in cash, which, after some deductions related to the expenses incurred and commission of the criminals in the form of the differences in exchange rates and a percentage of wire transfers, was sent back to the clients.

A subsequent police investigation of the business entities which used fraudulent primary accounting documents received from I. Ivanov and P. Petrov in order to avoid the payment of taxes and duties resulted in 7 criminal cases initiated under Art. 243 (evasion of taxes and duties) of the Criminal Code.

The following indicators of suspicious transactions were observed in the above scheme:

1. Low tax burden;
2. Minimum cash balances on accounts at the end of the trading day;
3. Employee strength of the front companies was 1-3 persons, including manager and accountant;
4. Reasonless splitting of amounts in identical transactions.

No typologies of money laundering involving the use of monetary instruments were detected by the Financial Monitoring Department. It should be noted that the popularity of financial instruments (bonds, bearer shares, traveler's checks, etc.) in Belarus has always been very limited.

Among measures designed to prevent illegal cash-out transactions carried out through the use of bank accounts of bogus entities that have be suggested by the Department are as follows:

- introduce a requirement for individual entrepreneurs who withdraw large amounts of money in cash (over 100 million BYR per month, which is equivalent to $11,764) to make an advance tax payment (income tax);

- oblige banks to charge a fee with a floating interest rate for all cash withdrawals – the higher the amount of withdrawn funds, the higher the fee.

- introduce a threshold on the amount and frequency of cash withdrawals by individual entrepreneurs and legal entities (no more than $2,000 per month);

- oblige the country's banks to break their dealings with entities suspected to be engaged in fictitious financial and economic activities and notify the financial monitoring body.

Cash-out transactions represent a threat to the normal functioning of the economy, while the money taken out of legal circulation are mostly used for criminal purposes.

Introduction of a rigid regulatory framework governing non-cash account transactions will greatly improve the current and subsequent monitoring of compliance by both bodies of executive power and banking institutions with the law.

According to the intelligence provided by our Russian colleagues, the most typical cash-out transactions in Russia involve the withdrawal of funds by:

- legal entities from their accounts through the bank cashier's desk for economic and other needs, payment of salaries, purchase of goods and materials;

- individuals through the bank's cashier's desk using checks, through ATMs of credit institutions using plastic bank cards (including cards registered under false name), through post offices in the form of remittances, such as Western Union.

The FIU of Russia provided examples of financial investigation into terrorist financing.

Example 1.

This investigation was preceded by the following events:

In September 2010, there was an explosion in one town located on the territory of the Republic of Ingushetia, which resulted in many casualties. A criminal investigation carried out in its aftermath resulted in the arrest of the mastermind behind the terrorist act, who happened to be Mr. X, one of the leaders of the illegal armed group called "Caucasus Emirate".

The searches of Mr. X's multiple premises yielded several computers with data on numerous companies, including their bank details.

A financial investigation began with the checking of these companies and revealed a possible terrorist financing scheme. One of the audited companies specialized in the supply of equipment to state enterprises and was headed by a close relative of Mr. X, his son. A close study of this company's activities revealed that only part of the funds received by it under a government contract for the supply of equipment was spent as intended, with another being cashed out and transferred to another one of Mr. X's close relatives, his brother.

Given the connection between the suspects and the armed gangs, the similar timings of the transactions and the terrorist act, and the discovered evidence of budget funds embezzlement, a decision was taken to refer the materials gathered to law enforcement. It should also be pointed out here that the funds found on the accounts of the identified relatives of Mr. X were subsequently seized.

Example 2.

While acting within its powers, the Federal Financial Monitoring Service carried out several checks on a number of individuals and legal entities linked to cross-border currency movement.

The emergence of this typology is largely due to Russia's decisive measures aimed at cracking down on illegal businesses specializing in cash-out transactions.

The cumulative amounts of transferred and cashed out assets involved in each overseas cash-out scheme can add up to several hundred million euro, with a scheme survival period ranging from several months to a year and a half - two years.

According to the Rosfinmonitoring, Estonia is the most popular country for overseas cash-out transactions. There are several reasons for this popularity:

• a large number of firms offering both currency exchange and cash-out services and not having the status of credit institutions (AS Tavid, AS Talvead, OU Instance, etc.);

• relatively low fees charged for the service;

• geographical proximity and, therefore, low cost of transporting the cash back to Russia;

• a large Russian-speaking minority, whose members share the same language and mindset with the residents of Russia and who traditionally belong to low-income groups and are willing to perform various non knowledge-intensive services, e.g. courier jobs.

Overseas cash-out schemes typically consist of the following stages:

Stage one.

Companies, and sometimes even individuals, specializing in cash-out services deposit their clients' funds into the accounts of registered fictitious entities (so-called "accumulators"), which keep track of the amounts deposited by each such client. Although only a single account is typically used to accumulate the funds of different clients, the tracking system used by the criminals allows them to see exactly how much each client has deposited, as if they were using different accounts. The account is managed remotely using the Client-Bank platform.

Stage two.

The collected clients' funds (both in rubles and other currencies) are then transferred by the accumulator companies on their own behalf and at their own expense either to:

their own accounts in foreign credit institutions, with "transfer of own funds" stated as the payment purpose;

or foreign companies' accounts (also registered in advance by the organizers of the illegal scheme), stating "under contract", "for services", "for securities", and other bogus reasons as the purpose of payment. The funds, in this case, may come to their accounts either directly from Russia or transit through the accounts of the controllable foreign entities opened in third countries.

Such foreign companies tend to be either registered in a country where the conversion of funds into cash is expected to take place (typically in Estonia),

or in a transit country between Russia and the same Estonia (Bulgaria, Kyrgyzstan, Latvia, Moldova, Ukraine and Finland),

or in an offshore jurisdiction (especially Belize and British Virgin Islands).

The beneficial owners of these entities are usually Russian nationals, who are also the organizers of the illegal financial scheme. The management of these foreign accounts is done online remotely, often with the use of specialized proxy software that hides the actual location of the host computer.

Stage three.

Once the funds have been transferred to foreign bank accounts, then they are either cashed out or moved to specialized exchange offices located in the same or a neighboring country for conversion into the desired currency and withdrawal. The Rosfinmonitoring has not detected any cases of overseas currency conversion resulting in cash withdraws made in rubles. This can be explained by the size- and value-related convenience of euro and dollar bills, as well as low currency fluctuation risks.

Stage four.

By using the services of couriers recruited from among the Russian and foreign nationals (in the case of Estonia, residents of the border towns of Ivangorod (Russia) and Narva (Estonia)), the scheme organizers smuggle the cash into Russia (typically in cars), where they distribute it among the clients who ordered the conversion services.

Financial transactions carried out during the first, second and fourth stages come within the scope of a definition contained in paragraphs 1-5 of Article 5 of the Federal Law #395-1 of December 2, 1990 "On banks and banking activity". All of the above transactions are subject to mandatory licensing by the Bank Russia and, therefore, can be classified as illegal banking activities, an offence covered by Article 172 of the Criminal Code of Russia.

That is, transactions of the first-fourth stages of the illegal scheme often involve the commission of a predicate offence.

The criminals' fees, expressed in several percentage points of commission for cash-out services, are collected either directly by the scheme organizers or through the controllable persons during the second or third stage (offence covered by Articles 174 and 174.1 of the Criminal Code of Russia).

These same stages also represent the first phase of money laundering – separation of proceeds from their criminal source.

For example:

at the second stage – accumulator companies transfer funds to the scheme organizer under various pretexts: payment for securities / services, return of loans, etc.;

at the third – while being controlled by the scheme organizers, foreign companies may transfer money to foreign accounts of the criminal scheme beneficiaries, or use it to pay for the purchase of real estate in other countries, yachts, cars, expensive jewelry, watches, etc.

According to the Russian FIU, the activities of the identified organizers of the scheme for cross-border movement of cash may constitute a predicate economic offence, namely: illegal banking activities (Article 172 of the Criminal Code of Russia), which are as follows:

With the goal of generating income and damaging Russia's economic interests by engaging in illegal banking activities on the territory of Russia, its beneficiaries use the services of the controllable companies registered using lost passports or under false name to open bank accounts for such entities in multiple banks.

Illegal activity is based on the establishment of illegal contractual relationships with various individuals and entities interested in taking advantage of illegal cash-out and conversion services, as well as in tax avoidance and channeling funds abroad.

To implement the above goals, the organizers of the illegal scheme abuse the existing banking system and violate the procedures and regulations governing it by transferring funds belonging to individuals and entities who ordered the above-described illegal services to the accounts of entities they control, for subsequent transfer abroad, withdrawal in cash, and return to Russia to their clients.

Thus, the above activities violate the Federal Law of Russia #395-I of December 2, 1990 "On banks and banking activity" (as amended) to the extent that the beneficiaries of the illegal scheme carry out illegal banking activities without registration and special permit (license) in cases where such permit is mandatory (Article 172 of the Criminal Code of Russia) by engaging in the following activities:

- raising funds by offering deposits to individuals and legal entities (par. 1 of Art. 5 of FL #395-I);

- managing the said raised funds on their behalf and at their own expense (par. 2 of Art. 5 of FL #395-I);

- collecting cash, provision of cash services to legal entities and individuals (par. 5 of Art. 5 of FL #395-I);

- purchase and sale of cash and non-cash foreign currency (par. 6 of Art.5 of FL #395-I).

Among the preventive measures designed to stem the flow of funds into the grey market and reduce the number of dubious cash transactions that are being suggested by our Russian colleagues is the need to promote a widespread use of non-cash payments by the public. In addition, in order to reduce the risk of money laundering through cash transactions, it is advisable to implement the following measures:

- strengthen the regulation and control over the circulation of bills of exchange in the country;

- block access to the financial system to bogus entities (entities that do not engage in any financial and real economic activity but, instead, are only established for use in illegal financial transactions) by adopting a number of appropriate legislative measures, e.g. a mechanism for blocking the accounts of shell companies and seizing funds deposited into them;

- increase the severity of sanctions applied against nominee heads and founders of shell companies (criminal liability, administrative liability) by making appropriate amendments to the legislation;

- ensure greater transparency with respect to limited liability companies in order to enable various rating and information agencies to rate the level of risk associated with each and every Russian legal entity (a good example of it is the Russian risk assessment company SPARK-Interfax);

- allow credit institutions to unilaterally refuse to perform the contract of bank account or deposit signed with the clients registered at mass registration addresses and blacklisted by the FTS of Russia;

- impose liability on individuals whose accounts are used for cash withdrawals.

Additionally, in order to reduce the risk of cash-out transactions being carried out using the cards registered under false name, it's necessary to begin using more sophisticated technologies that replace the authentication procedure for ATM users with an identification procedure, which allows transactions only by card owners.

According to the representatives of the Ukrainian Financial Monitoring Service, typical indicators of suspicious financial transactions involving cash and monetary instruments are:

1) purchase and sale of checks, traveler's checks or other similar payment instruments for cash;

2) crediting of funds in cash into an account and their subsequent same- or next-day transfer to another person;

3) carrying out financial transactions with bearer securities not deposited in depository institutions;

4) carrying out financial transactions with bills of exchange with blank endorsement or endorsement to bearer;

5) unusually intricate or confusing transactions, or transactions whose execution pattern is unusual, has no evident economic sense or obvious legal aim;

6) the financial transaction is not in keeping with the type and nature of the client's activities;

7) regular exchange of smaller notes against notes, especially in foreign currency, of higher value;

8) a substantial increase in the balance of account used to purchase bearer securities which is not associated with the activity of the legal entity or natural person (entrepreneur);

9) regular presentation of checks for collection issued by a non-resident bank and endorsed by a non-resident, where such activity is not in keeping with the legal or natural person's (entrepreneur) type of activities known to the reporting entity;

10) crediting by a natural person to the account of a legal entity or natural person (entrepreneur) of multiple amounts totaling no more than 150,000 UAH (13,000 UAH for gambling establishments), or equivalent or greater than the amount in foreign currency equivalent to 150,000 UAH (13,000 UAH for gambling establishments), including through a cashier's desk of the reporting entity, where the activities of the legal entity or natural person (entrepreneur) are not related to the provision of public services or the collection of mandatory or voluntary contributions;

11) a significant increase in the proportion of cash credited to the account of a legal entity or natural person (entrepreneur), where typical activities of the person typically involve cashless settlements;

12) crediting to the account of a significant amount of cash by a legal entity or natural person (entrepreneur) whose income level or occupation make it impossible for him to own such an amount;

13) transfer (or withdrawal) of funds in the amount of less than 150,000 UAH, where it was preceded by the crediting to the same account of cash in the amount equal to or greater than 150,000 UAH made during the same or previous working day;

14) carrying out transactions involving large amounts in cash, where the client's turnover is not large;

15) regular execution by a person of financial transactions with bills of exchange, if the person is not the issuer or payee of funds under these bills and is not a licensed professional securities market participant;

16) transfer of funds in cash abroad with a request to issue the funds to the recipient in cash;

17) regular crediting of funds to the client's account and their subsequent withdrawal in cash by him and/or his authorized representative;

18) regular withdrawal by the client and/or his authorized representative of cash previously credited to the client's account;

19) regular crediting of cash to the account of an individual or entity, provided it is not related to their core activities, followed by a transfer of the entire amount (or a larger part thereof) within one business day (or next business day) to:

- the client's account held in another reporting entity,

- a third party,

- a non-resident;

20) purchase by a person of public securities from a credit union for cash;

21) crediting by a person of large amounts in cash into deposit accounts held in banks or a united credit union;

22) early repayment of loans using large amounts in cash;

23) payment of the insurance premium in cash.

According to the intelligence provided by our colleagues from the Ukrainian FIU, the most typical cash-out transactions in Ukraine are:

For individual entrepreneurs and legal entities:

- withdrawal of funds to pay for goods and services, particularly for agricultural products;

- withdrawal of funds for economic or administrative purposes;

- withdrawal of business income;

- withdrawal of funds to finance the purchase of securities from individuals;

- issuance of loans/financial assistance to workers in cash .

For individuals:

- depositing and withdrawal of own savings;

- issuance of loans/financial assistance in cash.

The FIU of Ukraine has provided the following examples of schemes used for illegal cash-out transactions:

Example 1. Loan transactions.

Two insurance companies that share the same founders used a scheme for a rapid transfer of loan funds (with a difference of a few minutes) to the same contractor (A Ltd) as payment for securities, with subsequent conversion of non-cash assets into cash through natural person A.

Under this scheme, the insurance company A and insurance company B received in a single day 50 mln UAH of loan funds each from a bank at the end of a business day (at 18:50).

Immediately following that, the funds were transferred as payment for bills of exchange with special endorsement to the account of Company A Ltd.

In its turn, at 19:01, A Ltd transferred these funds in the amount of 100 mln UAH to the account of natural person A.

At 19:25, the funds were withdrawn in cash by natural person A.

It was also revealed that the bills issuer was bogus.

Natural person B, who is the founder of the insurance company A and insurance company B, as well as the insurance company A were involved in a scheme involving fraudulent activities in the property market.

Example 2. Deposit transactions.

Persons A and B placed 20 mln UAH each into deposit accounts of one banking institution.

On the same day, persons C and D received 20 mln UAH of loan money in cash each from the same banking institution.

Later the same day, these funds were paid back to the bank in cash by persons C and D as early loan repayment.

Also later the same day, persons A and B made early withdrawals of 20 million UAH in cash from their deposits.

Person A, according to the MIA records, was listed as a person in custody.

Person B had previously been convicted for drug trafficking.

Persons C and D were connected to one another (co-founders of two companies).

Example 3. Securities transactions.

With the goal of illegally converting non-cash assets into cash, a group of companies transferred over a four-month period 37.3 million UAH to an account of a securities dealer as payment of bills of exchange.

Subsequently, after receiving the funds, the securities dealer transferred the funds in their entirety during the same or next day to person A for shares issued by the company A.

In turn, person A withdrew these funds in cash during the same or next day through a bank cashier's desk.

A close study of documents revealed that:

- The founder of a securities dealer was person B, who in the past had been involved in running a conversion center;

- Person A is listed as unemployed. She is neither a business entity nor founder of any companies;

- Company A is a construction company. However, no information about this company's activities could be found in open sources (ownership of construction sites, equipment, assets, etc.);

- The subject matter of the contract for the sale of securities, under the terms of which the securities dealer had to transfer the funds for the benefit of person A, are bills or exchange and not shares;

- The shares issued by the company A are suspected to be fake given that a single share is priced at 4.3 UAH, which is more than 4 times above the nominal price;

- Given the slump experienced by the construction sector of Ukraine in 2010 and the lack of information about the Company A's activities, there is every reason to believe the share price is overinflated.

Example 4. Foreign trade transactions.

A non-resident company converts foreign currency in Ukraine and later withdraws them in cash.

The company G Ltd (Ukraine) and the company A (New Zealand) signed a contract for gratuitous financial assistance in the amount of 100 million euro.

Over a certain period, the company A credited the account of G Ltd with funds totaling 74.9 million euro and 27.5 million U.S. dollars (1bn UAH), part of which was immediately converted into national currency and withdrawn in cash through a bank cashier's desk by person B (the director of G Ltd) to finance the purchase of agricultural products in the amount of 77.4 million UAH.

The ensuing investigation revealed that person B was being investigated by law enforcement authorities for illicit production, acquisition, storage, transportation and delivery of narcotic drugs, psychotropic substances or their analogues without the intent to sell. This person was placed on the wanted list on suspicion of robbery and illegal entry into someone's home.

The intelligence provided by the FIU of New Zealand helped reveal that that the source of the funds in the accounts of the company A was the accounts of non-resident companies opened by Ukrainian nationals during a period of ten days.

The registered agent of the company A is the company S, which is suspected of engaging in activities related to registration of shell companies.

Conclusions and Suggestions

After summing up the results of the review of examples of money laundering schemes involving cash and monetary instruments, we can conclude that the reasons contributing to the risk of money laundering involving the use of these instruments are:

- poor quality of internal control measures in banks and non-bank financial institutions;

- insufficient level of reporting by banks and non-bank financial institutions of unscrupulous customers identified in the course of internal controls (as a consequence of the above reason);

- gaps in the relevant legislation that make the use of cash and monetary instruments for criminal purposes possible.

Disparity in the systems of control over the financial sector used in different countries. Adequacy of the measures applied is determined independently by each state based on past experience, as well as on the country's economic, geographical, historical and other metrics.

At the same time, in order to avoid or prevent the emergence of such schemes, it may be necessary to review the country's existing legal framework, assess the adequacy of the regulatory measures and effectiveness of monitoring mechanisms in place and, if necessary, consider their amendment, including in light of the new FATF recommendations.

In addition, particular attention should be paid to the establishment of permanent partnership relations with the private sector as an effective tool for identifying risks in different areas.

As a separate measure, it's is recommended to consider possible changes to applicable laws governing the circulation of currency and monetary instruments, which will make it possible to:

- lower to a safe level the threshold for cash withdraws by individual entrepreneurs and legal entities;

- introduce an obligation for legal entities and individual entrepreneurs to pay income tax when carrying out cash-out transactions above the threshold;

- introduce mandatory identification of persons discharging bearer monetary instruments and set limits on discharge of bearer monetary instruments;

- limit settlements between legal entities, as well as between legal entities and individuals, involving the use of monetary instruments.