ЕВРАЗИЙСКАЯ ГРУППА
по противодействию легализации преступных доходов
и финансированию терроризма

EURASIAN GROUP
on combating money laundering
and financing of terrorism

English – Or. Russian

REPORT

«Structural analysis of cash conversion-related financial flows associated with offences and money laundering»

Contents

INTRODUCTION

Relevance

Pursuant to the decision of the 24th EAG Plenary (June 2016) the typology research project entitled *Structural Analysis of the Financial Flows Linked to Encashment Transactions Used to Commit Crimes and Money Laundering* is implemented under the leadership of the Republic of Kazakhstan represented by the Financial Monitoring Committee of the Ministry of Finance of the Republic of Kazakhstan (hereinafter the FMC).

The project goal is to identify vulnerabilities of banks and non-bank financial institutions that require an increased focus on risks related to potential ML/TF transactions. The project also involves review of successful measures implemented for preventing conversion of criminal proceeds into cash. And finally, the project is aimed at developing typologies of the identified cash conversion-related financial flows associated with criminal offences and money laundering with the focus on the efforts undertaken by financial intelligence units (FIUs).

Main Objectives of the Project:

- Studying positive experience of countries in reducing share of cash transactions in general;
- Reviewing aspects that facilitate financial flows involving illegal funds;
- Analyzing cash conversion and money laundering typologies for their systematization and categorization;
- Elaborating recommendations on setting analytical tasks for information systems.

Target Audience:

The main users of the research product are financial intelligence units, reporting entities and law enforcement agencies of the countries.

Methodology:

For achieving the objectives of the research project, the Project Lead developed the Questionnaire which was disseminated to the EAG member countries, observers and international stakeholders.

The following EAG member countries provided the responses to the Questionnaire:

- Republic of Belarus;
- Republic of Kazakhstan;
- People's Republic of China;
- Russian Federation;
- Republic of Tajikistan;
- Turkmenistan;
- Republic of Uzbekistan.

The following EAG observer countries also took part in the research:

- Poland;
- Montenegro.

The Questionnaire is composed of 4 sections and includes 22 questions covering various aspects of the research topic. The questions are related to both the legislative and regulatory framework and practical cases and statistics maintained by the FIUs and LEAs.

Information from open sources was also used along with the received responses.

Research Outcomes:

It is planned that the research project will yield the following practical results: categorization of illicit cash conversion typologies; development of legislative preventive measures; and development of recommendations on setting analytical tasks for information systems.

1. GENERAL SITUATION WITH CASH CIRCULATION AND POSITIVE EXPERIENCE IN REDUCING SHARE OF CASH TRANSACTIONS

1.1 RESEARCH SUBJECT AND SCOPE

In this report, the term “cash conversion transaction” means financial transactions aimed at the withdrawal of non-cash money (or securities) from the banking system (from the securities market) by converting it into cash.

Illicit cash conversion is one of the urgent problems faced by most EAG member countries, since large quantity of uncontrolled cash facilitates the growth of shadow economy, feeds corruption and poses risk to economic security of the countries.

Quite often, large amounts of funds received as a result of cash conversion transactions are initially generated by economic offences, such as embezzlement and misappropriation of entrusted property (of budgetary funds), corruption, including bribery and “kickbacks”, and tax evasion by business entities.

Fake (fictitious) companies use a wide variety of tools for giving a legitimate appearance to ill-gotten money and further integrating it into the legitimate cash currency in circulation. Typically, funds are quite legitimately transferred to accounts of such companies. However, after funds are credited to their accounts, they carry out no business transactions, and no claims (or just minor informal claims) are laid against architects of these illegal schemes for failure to comply with contractual obligations. Schemes involving conversion of criminal proceeds into cash operate primarily through the banking system.

Today, sophisticated and broadly accessible financial services allow for making mutual payments and settlements within a short period of time after funds are placed into cash conversion and money laundering schemes.

Practical financial investigations show that cash conversion schemes have their own distinctive features and, therefore, may be subject to categorization.

Financial intelligence units (hereinafter FIUs) are capable of identifying cash conversion-related financial flows associated with criminal offences and money laundering by way of processing and analyzing data files related to financial transactions.

In general, there are 3 main components that are essential for generating cash conversion-related financial flows:

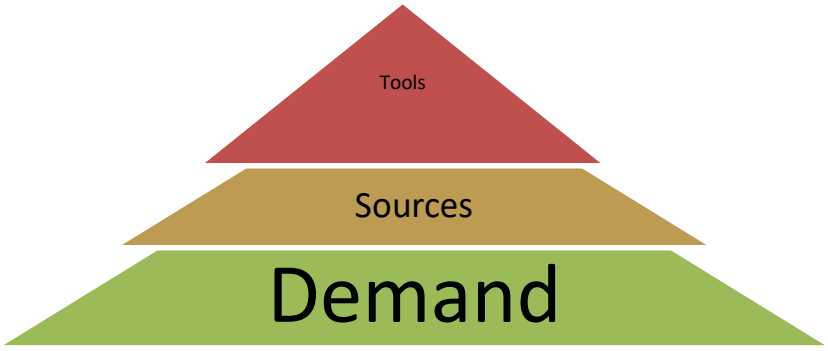
1) Reasons that cause high demand for cash;

2) Sources of cashless assets that are further converted into cash;

3) Tools and methods used for converting assets into cash.

In this context, this research considers aspects related to operation of the cash conversion market.

In this context, this research considers aspects related to operation of the cash conversion market.



The increased demand for large amounts of cash is the main reason for existence of the cash conversion market.

For the sake of clarity, factors generating high demand for cash may be divided into 3 categories, namely: **optimization of costs by business entities; accumulation of cash for paying bribes; and concealment (laundering) of criminal proceeds.**

Business entities traditionally use cash for the cost optimization purposes in order to decrease their taxable income and reduce costs related to purchase of goods and performance of work. This enables companies to gain advantage over competitors in the market. Payment for goods and work is made in cash, typically, at lower prices, low-paid manpower is hired for performing work, and envelope wages are paid to employees.

At the same time, there is some evidence that another factor that generates increased demand for cash in the developing countries is the need to pay bribes to corrupt officials, who, according to the law enforcement agencies, prefer to receive bribes in cash.

The main reasons for this are the advantages of cash, which is highly liquid in the market, entitles the holder rights of ownership, and is easily convertible into other movable/ immovable assets. Besides that, unlike cashless transactions, no commission/ fee is charged for cash payments. In the expert opinion, need to pay "kickbacks" is today one of the main factors that generates high demand for cash. Thus, the corruption factor plays the most significant role in cash demand.

In addition to that, demand for converting cashless assets into cash may also be caused by need to launder proceeds obtained through crime. In most cases, such criminal proceeds are generated by various criminal offences committed against property of individuals/ legal entities (*theft, misappropriation, fraud)* as well as by distribution of narcotic drugs and other prohibited substances. It is very difficult to estimate the level of such demand, since these particular transactions are hardly distinguishable from other large volume cash conversion transactions. However, some LEAs believe that volume of criminal proceeds illegally converted into cash is significantly lower that the volume of cash proceeds obtained through tax offences and corruption-related crimes that generate high demand for cash.

Assets may also be converted into cash for financing of terrorism. However, this type of criminal activity is not considered in this report as the cash demand generating factor, since volume and value of these transactions are incommensurably low compared to the aforementioned factors. TF-related cash conversion transactions are featured by occasional and targeted nature.

At the same time, funds intended for terrorist financing may originate from criminal activity and, therefore, may be referred to the 3rd factor that generates demand for cash conversion services.

Typical sources of funds that are illegally converted into cash in the Eurasian Region countries may be divided into 3 groups: **state budgetary funds; non-budgetary commercial revenues of business entities; and funds obtained through crime.**

The volumes of budgetary and non-budgetary funds can hardly be estimated. However, given the business development trends, the experts share the view that the budgetary funds currently prevail over the commercial revenues in the CIS member countries. Moreover, large companies often generate their revenues, *inter alia*, by using funds allocated from the state budget.

In particular, business entities in the Kazakh Republic depend heavily enough on volume of public procurement contracts awarded to them. In this context, it is highly probable that budgetary funds prevail over funds from other sources.

The international experts note that there is a direct link between shadow economy and corruption, one of the consequences of which is emergence of cash conversion schemes disguised as subcontracting arrangements.

Conclusions:

The "cash conversion" phenomenon has emerged and exists as a result of high demand factor due to undeniable advantages of holding funds in cash form.

Reduction or elimination of cash conversion activity is a comprehensive and complex task which involves improvement of various areas of government regulation, including AML/CFT, tax

administration, public procurement and anti-corruption policy.

The research also includes review of the legislation governing the AML/CFT and banking regulation issues and considers the legislative restrictive and preventive measures.

The overriding priority of countries that face this problem is to disrupt and eliminate illegal cash conversion schemes. However, since this problem covers multiple financial and economic aspects of the government activity, mere imposition of strict limitations and restrictions will not resolve the problem.

At the same time, the experience gained by the countries shows that implementation of certain measures enables them to reduce risks of abuse of financial institutions for illicit cash conversion purposes.

In general, the government anti-cash conversion policies pursued by the surveyed countries include, among other things, development and promotion of cashless payments methods. This will enable to increase transparency of business entities operating in the national market and also to "red flag" the cash intensive sectors that are exposed to the highest risks.

1.2 GOVERNMENT REGULATORY MEASURES

Most countries take measures for promoting cashless payments.

The surveyed countries implement similar regulatory measures for promoting cashless payments:

1) The countries take measures for popularizing and spreading cashless means of payment, such as debit cards, credit cards and other cashless payment instruments;

2) Certain types of private sector entities are required to install payment terminals for accepting payments for goods and services with the use of electronic means of payment;

3) The legislation of individual countries imposes limitations on use of cash for making payments and settlements between/among legal entities:

Country	Limitation
Republic of Kazakhstan	1,000 monthly calculated indices *
Republic of Belarus	100 base units per day **
Russian Federation	100 000 Rubles
Poland	15,000 euro

* Monthly calculated index is equal to KZT 2,269 in 2017;

** Base unit is equal to BYN 21.

At present, the legislation of most countries that take part in the research, impose no restrictions on amount of cash that can be withdrawn from bank and other accounts, except for situations when cash desks and automated teller machines run out of cash.

In the **Republic of Kazakhstan**, no restrictions are imposed on cash withdraws from bank or other accounts, except for situations when banks' cash desks run out of cash.

The similar situation is in **Poland, Republic of Tajikistan and Russian Federation** – no strict regulations pertaining to withdrawal of cash from bank accounts are established.

Credit institutions themselves establish cash withdrawal limits in line with their internal regulations and instructions. However, credit institutions are obliged to conduct CDD and file a report when transaction amount exceeds the established threshold.

In the **Russian Federation**, unlimited amount of cash may be issued to customers from their bank accounts provided that it does not exceed the account balance, unless otherwise is stipulated in a bank account agreement. However, according to clause 2.5 of BoR Regulation No.266-P of December 24, 2004 on Issuing Payment Cards and Carrying Out Transactions with the Use of Payment Cards:

It is recommended to an issuing credit institution to allow the aforementioned customers to withdraw the Russian currency cash in amount not exceeding RUR 100,000 during one operational day. However, the applicable laws and regulations do not oblige an issuing credit institution to

impose the relevant cash withdrawal limits for individual customers (natural persons).

Pursuant to the applicable legislation of the **Republic of Uzbekistan** only cashless payments can be made between/among legal entities and natural persons involved in entrepreneurial activities.

Payments between/ among the aforementioned persons may also be made in cash, unless otherwise is provided for by the law. In particular, according to Article 21 of the Law of the Republic of Uzbekistan on Guarantees of Freedom of Entrepreneurship funds held in bank accounts of individual entrepreneurs may be withdrawn in cash in a manner established by the legislation. Besides that, Clause 5 of the Regulation on Cash Transactions Carried Out by Legal Entities stipulates that cash withdrawn by business entities from their bank accounts may be used only for those purposes for which it is withdrawn.

It is of particular interest to mention the experience of some countries which **legislation imposes restrictions** on withdrawal of cash from bank accounts.

In the **Republic of Belarus**, the amount of cash that may be withdrawn by business entities from their accounts is limited by 100 base units per day for making cash payments to other business entities (the base unit is equal to 21 Belarusian rubles).

Limits are also established in **Turkmenistan**. The maximum amount of cash that may be withdrawn by legal entities and individuals from their accounts opened with banks located in Turkmenistan is limited by TMT 35,000 (Turkmen manats) per month.

The legislation of **Montenegro** imposes limitations with consideration for the established amount of maximum cash balance in hand.

In particular, legal persons and entrepreneurs may, in the course of the day, use cash to pay for goods and services, provided that they may keep cash in hand at the end of the day up to the amount of maximum cash balance.

The maximum cash balance amounts to:

- *for small legal persons and entrepreneurs - up to 2,000 euros;*
- *for medium-sized enterprises - up to 10,000 euros;*
- *for large enterprises - up to 20,000 euros.*

Legal persons and entrepreneurs are obliged to pay cash into their account in the amount that exceeds the maximum cash balance until the end of the working day, but not later than the next working day by 14:00. Small, medium and large enterprises mentioned above are considered legal persons classified in accordance with the law governing accounting and auditing. The legislation of Montenegro prescribes penalties for the failure to comply with the aforementioned obligations by legal persons and enterprises.

Conclusions

The comparative analysis of the information on general situation with cash circulation received from the countries participated in the research allows for making a conclusion that, in general, the countries pursue similar policies for promoting cashless payments:

1) The countries take measures for popularizing and spreading cashless means of payment, such as debit cards, credit cards and other cashless payment instruments;

2) The countries required certain types of private sector entities to install payment terminals for accepting payments for goods and services with the use of electronic means of payment;

3) The legislation of individual countries imposes limitations on use of cash for making payments and settlements between/among legal entities. Such limitations are apparently established, to a greater or lesser extent, in most countries.

The legislative limitations on cash withdrawals vary across different countries that took part in the research.

No cash withdrawal limits are established in Kazakhstan, Poland, Tajikistan, Russia and Montenegro. In China, the daily limit on the amount of cash withdrawal from ATM is CNY 20,000 and the institutions shall make transfer through bank accounts for business transaction except the use of cash falls within salaries, etc.

The legislative limitations on cash withdrawals are imposed in Belarus and Turkmenistan.

Based on the countries' responses, it can be concluded that such limitations, in fact, enable to mitigate risks related to integration of criminal flows into legitimate circulation through cash conversion transactions.

1.3 RISK ASSESSMENT DURING GOVERNMENT REGISTRATION OF COMPANIES

At present, the government institutions of the surveyed counties do not apply any special measures for assessing risk of legal entities at the stage of their government registration.

In particular, the **Republic of Kazakhstan** has no effective mechanism in place for preventing establishment of fake (fictitious) companies at the stage of government registration (re-registration) of legal entities, since the simplified registration procedure is used and minimum set of documents (application and ID documents of a founder) is required for registration, which provides the favorable business registration and operation regime. In particular, instruments of incorporation may be submitted to the registration authorities (justice authorities) not only be a founder, but also by his/her authorized representative, which makes it much easier for criminals to achieve their malicious goals. Besides that, registration of a legal entity does not involve inspection of its legal address.

In general, similar situation exists in other surveyed countries.

In our opinion, establishment of a mechanism for assessing risk of newly established business entities would enable to identify fictitious (fake) parties to financial transactions as risky ones at the government registration stage and to notify financial institutions of the need to pay special attention and apply enhanced due diligence measures in respect of such entities.

The provided responses show that legislation of some countries provides the grounds for denying government registration of legal entities in certain circumstance (where certain conditions are not met):

1) According to the Law of the **Republic of Kazakhstan** on Government Registration of Legal Entities and Record Registration of Branches and Representative Offices the government registration (re-registration) of legal entities is denied, *inter alia*, in the following situations:

- if a legal entity or a sole founder (member) of a legal entity is a dormant (inactive) legal entity;

- if a natural person, who is the founder (member) and (or) the head of a legal entity, is the sole founder (member) and (or) the head of dormant (inactive) legal entities, and (or) was recognized incapable or partially capable, and (or) was declared missing, and (or) was declared dead, and (or) has a non-discharged record of conviction for committing criminal offences covered by Article 237 (Illegal Actions upon Rehabilitation or Bankruptcy), Article 238 (Premeditated Bankruptcy) and Article 240 (Bankruptcy Fraud) of the Criminal Code of the Republic of Kazakhstan, as well as in case if the founder (a natural and (or) legal entity), the head of the legal entity, the founder and (or) the head of the legal entity who established the entity, is the debtor under an executive document, except for the entity being the debtor under an enforcement procedure for recovery of periodic payments and not having arrears on the enforcement procedure for periodic collection for more than three months;

- if lost and (or) invalid ID documents are submitted;

- if there are acts and orders (bans, arrests) issued by court enforcement officers and LEAs.

2) According to the **Turkmen** Law on Companies government registration of a company may be denied, *inter alia*, if there is information available indicating that founders, senior managers or ultimate beneficiaries are involved in criminal activity, or have a non-discharged record of conviction.

3) The legislation of the **Russian Federation** provides for measures that shall be taken for verifying veracity of information on legal entities and individual entrepreneurs.

In particular, according to paragraphs 4.2 and 4.4 of Article 9 of Federal Law No.129-FZ on Government Registration of Legal Entities and Individual Entrepreneurs dated August 8, 2001 (hereinafter Law No.129-FZ) the registration authorities are obliged to verify veracity of information that is being and has been recorded in the Single State Register of Legal Entities (SSRLE) if they have reasonable doubts about the veracity of such information.

If following verification of veracity of information recorded in the SSRLE, such information is found to be false, the government registration is denied.

Besides that, if verification of veracity of information that has been already recorded in the SSRLE reveals that such information is false, the relevant record is made in the SSRLE, which is accessible for all stakeholders.

Moreover, Article 23(1)(ф) of Law No.129-FZ imposes restrictions for natural persons through whose fault inaccurate (false) information has been recorded in the SSRLE, thereby ruling out the possibility of creation by such natural persons of new legal entities that pose high risk of being misused for illegal activities.

Conclusions:

The laws governing government (state) registration of legal entities provided by the surveyed countries show that safeguarding the rights and freedoms of business entities is the top priority in line with the Constitution and other fundamental legislative acts.

Furthermore, immunity is granted to individuals and entities provided that they have discharged all obligations towards the State, i.e. served imposed sentences, paid levied monetary fines, etc.

Alongside with that, it is expedient to consider and adopt the **practice of the Russian Federation** related to verification of veracity of information that is being and has been recorded in the state register of legal entities if there are reasonable doubts about adequacy and accuracy of such information.

Given that legal entities with nominee directors are often used for carrying out transactions involving conversion of criminal proceeds into cash, it is also advisable to develop a mechanism that would enable to identify high-risk entities that most likely use nominee (dummy) directors and executive officers at the stage of their government registration.

Besides that, the legislation of some countries imposes criminal liability for registration of business entities in the name of front persons who are actually not involved in operation of such entities.

In general, introduction of a mechanism for assessing risk of legal entities at the stage of their government registration is not a new idea. However, no balanced and efficient mechanisms have been implemented internationally so far.

As for preventive measures, the received responses often mention criminal intelligence and detective measures taken by LEAs for identifying and targeting fake (fictitious) companies. Although this mechanism enables to identify high-risk business entities, it is too narrowly focused and, therefore, does not ensure nationwide mitigation of risks associated with creation and operation of fake (fictitious) companies.

On the other hand, the legislation of most surveyed countries provides for forced liquidation of legal entities that meet certain fictitious criteria. However, the forced liquidation procedure (often by court order) is more complex and challenging in practice, compared to voluntary liquidation/ dissolution.

In this context, it is proposed for the countries to consider introduction of a simplified procedure of liquidation of legal entities that meet fictitious criteria.

It is also suggested to develop a mechanism for identifying registered fake (fictitious) companies by updating the state registers of legal entities based on certain criteria.

1.4 CUSTOMER DUE DILIGENCE AND RISK ASSESSMENT

As for customer due diligence (CDD), all surveyed countries apply enhanced CDD measures where there are factors indicating high risk posed by customers and their transactions. Such risk factors may be set out in the AML/CFT legislation and/or may be developed by obliged entities themselves with the application of a risk-based approach.

In most cases, the enhanced CDD procedures implemented by entities that are subject to

financial monitoring are very similar across the surveyed countries.

Banks perform **standard, simplified** or **enhanced** identification of a customer (and beneficial owner), depending on a degree of risk posed by such customer.

The circumstances where enhanced identification is required are set out in the national laws and regulations.

When applying enhanced CDD measures, entities that are subject to financial monitoring take one or more of the following actions, in addition to due diligence:

1) Establish reasons for intended or performed transactions;

2) Increase number and timing of controls applied and select patterns of transactions that require further examination;

3) Obtain senior management approval to establish and/or continue business relationships with customers.

The financial investigation practice shows that one-time customers that are subject to enhanced CDD often demonstrate good knowledge and understanding of industry-specific AML/CFT regulations, which allows them to carefully plan in advance their actions and responses in case they raise banks' suspicion.

Example: modus operandi of a customer involved in cash conversion transactions

According to a pre-designed scheme "shadow" companies open multiple current accounts with different banks. After carrying out cash conversion transactions for a certain period of time, the customer is included in the list of customers posing increased ML/FT risk.

After that, the bank requests the customer to provide additional information and documents to determine whether the customer poses enhanced or reduced risk.

Should the customer fail to provide such additional information and documents, the bank may refuse to carry out transactions, suspend transactions or terminate business relationship with the customer.

However, since "shadow" companies know the mechanism used for identifying high-risk customers, they voluntarily terminate the business relationship with the bank and switch to a different bank. In doing that, they are typically allowed to transfer the account balance to a new account opened with a different bank without any impediments.

The drawback of this high-risk customer identification mechanism is that information on a customer risk remains locked away in just one bank and is inaccessible to other banks for applying preventive measures.

In this context, a consideration should be given to development of a mechanism for sharing such information among reporting entities to enable them to take preventive measures.

However, the Russian and Belarusian legislation is featured by certain specificities related to identification of high-risk individual/ corporate customers by reporting entities that are worth mentioning.

In the **Republic of Belarus**, the preventive measured taken by entities engaged in financial transactions in the process of customer identification involve cross-checking of customers against the list of business entities and individual entrepreneurs posing enhanced risk of economic offences, as prescribed by RB Presidential Decree No.488 of 23.10.2012 on Certain Measures for Preventing Illegal Minimization of Tax Base.

The **Russian Federation** has the mechanism in place for sharing information by way of reporting the relevant information to the government regulator.

Article 7(13) and (13.1) of Federal Law No.115-FZ requires entities engaged in transactions with funds or other assets to document and report to the designated agency (Rosfinminitoring) about all instances when they refuse to carry out transactions, refuse to establish business relationships and (or) terminate business relationships, inter alia, due to suspicions that a transaction is carried out (business relationship in established) for ML/TF purposes.

Rosfinmonitoring, in turn, disseminates such reports received from entities engaged in transactions with funds or other assets to the Bank of Russia.

And, the Bank of Russia issued Regulation No.550-P of July 20, 2016 on "Procedure of

communicating information about instances of denied transactions and denied and/or terminated bank (deposit) account agreements to credit and non-credit financial institutions".

Conclusions:

The analysis allows for drawing a conclusion that the enhanced CDD measures applicable in the surveyed countries are implemented in a similar manner.

As for the improvement of mechanisms used for examining and assessing customer risks, it is expedient to enable entities that are subject to financial monitoring to share information on high–risk customers with each other in order to develop the national preventive system for identifying and preventing operation of "shadow" companies involved in cash conversion transactions.

Currently, the legislation of the surveyed countries, except for the Russian Federation, does not provide for direct exchange of information on high-risk customers among entities that are subject to financial monitoring.

In the context of globalization, and also taking into account the widely spread shadow schemes used for converting criminal proceeds into cash, a consideration should be given to possible extension of international cooperation and exchange of information on high-risk customers involved in cross-border transactions in future.

It is worthwhile to mention the positive experience of the Russian Federation related to centralized exchange of information by way of informing the government regulator about all instances when entities engaged in transactions with funds or other assets refuse to carry out transactions, refuse to establish business relationships and (or) terminate business relationships, *inter alia*, due to suspicions that a transaction is carried out (business relationship in established) for ML/TF purposes.

1.5 AUTHORITY OF ENTITIES TO CARRY OUT CASH TRANSACTIONS

Listed in the Table below are the types of entities that are subject to financial monitoring operating in the surveyed countries with indication whether or not they are authorized to carry out cash transactions.

	Kazakhstan	Uzbekistan	Turkmenistan	Tajikistan	Poland	Russia	China
Insurance and mutual insurance companies	●		●	●	●	●	●
Pension funds	●				●	●	
Mirco-finance organizations	●	●		●	●	●	●
Third-party payment processors *	●	●	●	●	●	●	●
Gambling and lottery operators	●			●	●	●	

* - also include operators of money transfer systems (including e-money operators)

In the **Republic of Kazakhstan**, the National Bank regulates, oversees and supervises financial institutions (banks, non-bank institutions, insurance companies, the unified pension savings fund, voluntary pension savings funds, securities market entities and micro-finance organizations) as well as third-party payment processors that fall into the category of entities that are subject to financial monitoring.

All entities listed above are authorized to carry out cash transactions.

It is noteworthy that certain constraints are imposed on insurance agents – Article 18(4) of the Law on Insurance prohibits an insurance agent from accepting cash from an insured party as payment of the premium when entering into insurance contract on behalf or at the direction of an insurance company.

However, this constraint does not apply to situations where insurance agents accept cash, at

the border checkpoints, as payment of insurance premium under insurance agreements from persons visiting Kazakhstan.

The terms and conditions of business relationships between financial institutions and their customers are set out in the respective agreements entered into by the parties.

In the **Russian Federation**, all entities engaged in transactions with funds or other assets and individual entrepreneurs that are fully covered by the AML/CFT legislation are authorized to carry out cash transactions.

Non-credit financial institutions that are regulated, monitored and supervised by the Bank of Russia in compliance with Article 76.1 of Federal Law No.86-FZ of 10.07.2002 on the Central Bank of the Russian Federation (Bank of Russia) and are subject to the RF AML/CFT legislation, that may accept cash payments when providing respective financial services, include:

- *Professional securities market entities;*
- *Insurance companies (except for medical insurance institutions that issue mandatory medical insurance policies) and insurance brokers;*
- *Mutual insurance companies;*
- *Investment fund, mutual investment fund and non-government pension fund management companies;*
- *Non-government pension funds licensed to provide occupational pension and insurance services;*
- *Consumer credit cooperatives, including agricultural consumer credit cooperatives;*
- *Micro-finance organizations;*
- *Pawnshops.*

Section 1 conclusions:

The provided responses show that no strict constraints on customer cash transactions carried out by entities that are subject to financial monitoring are imposed in Kazakhstan, Russia and Poland.

Other surveyed countries impose limitations on cash transactions.

In the framework of this study, it is impossible to elucidate the potential impact of permitted cash transactions on the overall national risk of misuse of such transactions for cash conversion purposes.

In particular, the analysis of preliminary assessment of risks associated with use of cash for ML/TF purposes presented below in this Report indicates that no links between imposed limitations and risk reduction have been revealed.

At the same time, it is noted that, today, cash generated as a result of distribution of goods and provision of services by business entities is commonly offered for sale by operators of cash conversion schemes.

Example of cash sale scheme without involvement of financial institutions

Ordering parties (who order cash) transfer non-cash money to the scheme operators supposedly as payment for goods, work and services, and the latter return uncollected cash (which they are obliged to deposit into bank accounts) net of commission fee to the ordering parties.

Such schemes may be arranged by large construction materials retail networks, petrol station networks, large consumer goods retail companies, etc. Operators of such schemes use the received non-cash money for making payments to their suppliers.

Thus, these cash sale schemes operate without any need for carrying out cash conversion transactions through financial institutions. Quite often, amount of cash generated through such schemes is comparable to the volume of cash withdrawn from bank accounts by illegal cash conversion service providers. Actually, shadow cash sale scheme operators act in the capacity of banks offering teller transaction services to the customers.

Therefore, cash may originate from both financial/non-financial institutions and retail networks that generate large amounts of cash through sale of goods, performance of work and provision of services.

In such circumstances, the governments realize the need for promoting cashless payments,

since the significant portion of cash is generated as a result of payments for goods and services by the general public.

At the same time, in the context of globalization of the economic processes, the countries (in particular, the Republic of Kazakhstan) have taken measures aimed at liberalization of the legislation in order to minimize the negative impact of administrative barriers on free movement of capital for promoting business activities and improving the domestic investment climate.

In this situation, it is obvious that the countries need to strike a reasonable balance between the government and business interests for minimizing risks of laundering and integration of criminal proceeds into the legitimate economy through misuse of cash transactions.

However, the private sector should understand and be ready to operate in a transparent and open manner such as to be fully accountable to the government.

2. FIU ACTIVITY, CAPABILITIES AND ANALYSIS

2.1 ALGORITHM OF ASSESSMENT OF RISKS OF SUSPICIOUS TRANSACTION REPORTS FILED WITH FIU

The provided responses show that all FIUs use the internal automated procedures for assessing risk of incoming reports.

Automated (online) access to external databases is the undisputable advantage of the risk assessment systems.

In particular, in the **Republic of Uzbekistan**, the FIU performs comprehensive automated examination and analysis of incoming reports, which involves cross-checking against the relevant databases (lists) of:

- *legal entities and individuals that are involved or suspected of being involved in terrorist activity;*
- *legal entities and individuals that directly or indirectly own or control an organization that is involved or suspected of being involved in terrorist activity;*
- *legal entities that are owned or controlled by an individual or organization that is involved or suspected of being involved in terrorist activity;*

In addition to that, the Uzbek FIU performs automated checks:

- *checks against passport database;*
- *checks against travellers entry/exit database;*
- *checks availability of earlier filed reports related to a particular entity/ individual;*
- *checks against other available databases (export/import of goods, information on account activity, data from real estate property register, etc.).*

After that, a conclusion is made about nature of a suspicious transaction and parties thereto based on the received initial information.

When found appropriate, additional intelligence on a suspect is gathered and examined and, in case of a positive match, a case file is prepared and submitted to the relevant agencies.

The FIU of the **Republic of Belarus** has developed a special software system that enables it to perform multi-criteria analysis of STRs, which includes assessment of reports, including previous reports, and assessment of parties to suspicious transactions.

Likewise, the FIU of the **Russian Federation** has implemented the risk assessment algorithm based on incoming STR flow, including analysis of previously filed reports. In fact, this mechanism involves comprehensive algorithmic assessment by the relevant departments of the FIU of STR-related entities, such as legal entities/ individuals, transaction originators/ recipients, accounts used, credit institutions, etc.

Thus, all STR-related entities are grouped into a cluster of relationships, to which appropriate risk level is assigned by the relevant government agencies. And conversely, array of such clusters provides the opportunity for integral assessment of both a transacting party (e.g. identification of fictitious nature or engagement in shadow business, based on results of financial investigations) and

a credit institution involved in a transaction.

The information and analytical environment of the Russian FIU enables it to use the risk assessment results for generating targeted and macro-analytical aggregated data that allow for identifying high risk concentration areas in the process of operational (daily), tactical (monthly/ quarterly) and strategic (annually) analysis and allocating resources (analysts) accordingly to address the routine problems.

The **Republic of Kazakhstan** uses the Operational Analysis subsystem that ranks the incoming STR.

The Operational Analysis module analyzes the reports submitted to the national AML/CFT database for identifying suspicious indicators and red flags.

In addition to the indicators/ red flags, the table for ranking STRs according to each indicator has been developed.

Upon detection of any indicator, the Operational Analysis module assigns the relevant suspicion rating to the report.

If several indicators are detected, the total suspicion rating is calculated by adding all ratings assigned based on each individual indicator.

The results of assessment of incoming reports performed by the Operational Analysis module are used for compiling the list of the most risky transactions that require prioritized examination.

One of the distinctive features of the Operational Analysis module is that it analyzes transactions against historical data.

The list of indicators and red flags for identifying transactions that pose the highest risk is adopted by the internal regulations of the Kazakh Financial Monitoring Committee.

Conclusions:

The provided responses show that the surveyed countries implement and use the software systems with multi-criteria analysis capabilities. Quite often, the FIUs have access to a broader range of information than just multiple reports submitted to the FIU databases in compliance with the AML/CFT legislation.

The available information sources include the following:

- *databases containing information on natural persons;*
- *databases containing information on legal entities;*
- *databases containing records of births, deaths and marriages;*
- *tax databases;*
- *customs databases;*
- *other*

As regards effectiveness of the efforts undertaken by the FIUs, access to a broad range of information enables them to more effectively assess risks of incoming reports using the capabilities of their information systems and implementing automated data processing technologies.

According to subsection 6 of the Interpretive Note to FATF Recommendation 29 in order to conduct proper analysis, the FIU should have access to the widest possible range of financial, administrative and law enforcement information. This should include information from open or public sources, as well as relevant information collected and/or maintained by, or on behalf of, other authorities and, where appropriate, commercially held data.

However, it should be noted that access to the national databases using a request-response communication pattern does not allow for improving, to the maximum possible extent, effectiveness of analysis of a full range of information submitted to the FIUs.

To this end, it is obvious that information from other databases should be accumulated in the FIUs' databases and kept up-to-date for conducting financial investigations.

The practice shows that many FIUs still face challenges in accessing their national databases or may obtain information only at request.

2.2 POWERS TO SUSPEND SUSPICIOUS TRANSACTIONS

Statutory powers of the FIUs to suspend suspicious transactions are one of the mechanisms used for preventing integration of criminal cash flows into legitimate circulation.

According to the provided responses most FIUs are authorized to suspend suspicious transactions and deals.

	Powers of FIU to suspend (freeze) transactions
Kazakhstan	●
Uzbekistan	●
Belarus	●
Turkmenistan	●
Montenegro	●
Poland	●
Russia	● [1]
Tajikistan	*NA*

Powers and methods used for suspending (freezing) transactions in line with FATF Recommendation 4 vary across different countries.

According to Recommendation 4 countries should adopt measures similar to those set forth in the Vienna Convention, the Palermo Convention, and the Terrorist Financing Convention, including legislative measures, to enable their competent authorities to freeze or seize and confiscate the following, without prejudicing the rights of bona fide third parties: (a) property laundered, (b) proceeds from, or instrumentalities used in or intended for use in money laundering or predicate offences, (c) property that is the proceeds of, or used in, or intended or allocated for use in, the financing of terrorism, terrorist acts or terrorist organizations, or (d) property of corresponding value.

The received responses show that most FIUs are authorized to suspend (freeze) suspicious transactions.

However, it is assumed that in situations, where the legislation does not impose cash conversion constraints and where there are high risks of use of cash for ML/TF purposes, suspension (freezing) of transactions may be inefficient for preventing illegal cash conversion, since most FIUs are empowered to suspend ML-related suspicious transaction for no longer than 3-5 days.

For example, the mechanism used for suspending suspicious transactions potentially related to laundering of tax crime proceeds in no way helps to disrupt illegal cash conversion activities, since in order to institute a criminal case the LEAs need to obtain the resolution or order from the relevant authorities, which takes at least 1 or 2 months, while the average period for which FIUs can suspend transactions does not exceed 3-5 days.

It is obvious that in order to improve effectiveness of the transaction suspension mechanism used by the FIUs, the law enforcement and tax authorities should be able to further extend the transaction suspension period.

In practice (in particular, in the Republic of Kazakhstan), the LEAs may impose further limitations on transactions (extend transaction suspension period) only upon obtaining the relevant court order after institution of a criminal case.

In our opinion, suspension (freezing) of suspicious transactions by the FIUs may have the maximum effect, if such suspension is preceded by a financial investigation conducted by FIU, *inter alia*, jointly with the law enforcement agencies.

In a situation featured by high risks of use of cash for ML purposes, the efforts should be focused, first of all, on establishing roots and causes which facilitate generation of criminal proceeds that are further laundered by criminals and, after that, on development of preventive measures.

[1] Transactions with funds or other assets carried out by organizations or individuals that are known to be linked to extremist activities or terrorism, or by legal entities that are directly or indirectly owned or controlled by such organizations and individuals, or by natural or legal persons acting of behalf or at direction of such organizations or individuals.

Thus, mere suspension of suspicious transactions by FIU without further imposition of limitations by the law enforcement and tax authorities cannot be deemed effective for mitigating national ML/TF risks.

2.3 RISKS OF USE OF CASH FOR ML PURPOSES

The surveyed countries were requested to give a tentative assessment of degree of risk associated with use of cash for money laundering purposes.

The received responses were used for compiling the following Table that presents preliminary assessment of risk degree.

Country	Risk of Use of Cash for ML Purposes *
Kazakhstan	Medium / High
Belarus	Medium
Turkmenistan	Low
Montenegro	Medium
Russia	High
Tajikistan	Low
China	Medium
Uzbekistan	*NA*

* - Preliminary assessment of risk of use of cash for ML purposes based on subjective opinion of FIUs and relevant government authorities

The Table shows that assessment of risk degree varies across the surveyed countries. There does not seem to be a direct connection between legislative constraints on cash transactions and risk of use of cash for ML purposes. However, Kazakhstan and Russia, which do not impose strict limitations, assessed the risk as medium high and high, respectively.

The presented assessment is subjective in its nature, and such assessment should be conducted in the framework of the national risk assessment (NRA) with involvement of all relevant government stakeholders. The main purpose of NRA is to develop preventive measures for mitigating risks of misuse of the national financial system for ML/TF purposes.

The global trends related to application of a risk management approach have become widespread and are used as the important element of the anti-money laundering and counter-terrorist financing system. The risk-based approach is one of the core elements of the FATF Recommendations and is elaborated in Recommendation 1.

National ML/TF risk assessment is an important step towards efficient and effective combating money laundering and terrorist financing in the EAG member countries.

2.4 PERCENTAGE OF FINANCIAL INVESTIGATIONS RELATED TO CASH CONVERSION AND WITHDRAWAL

Number of financial investigations into cash withdrawal transactions varies significantly across the surveyed FIUs.

For example, in **the Republic of Kazakhstan**, financial investigations into cash conversion/withdrawal transactions accounted for approximately **80%** and nearly **90%** of all financial investigations conducted in 214 and 2015, respectively, while only **13%** of financial investigations conducted by the **Uzbek FIU** in 2014-2015 were related to cash conversion and cash withdrawal transactions.

Since cash conversion and withdrawal may be part of the money laundering process used for separation of criminal proceeds from the underlying offences and their further concealment, the use of cash by suspects is observed in **most financial investigations** conducted in the **Russian Federation**.

Interestingly, according to the information provided by **Turkmenistan no financial transactions related to cash conversion and cash withdrawal transactions were registered** in the country in 2014-2015.

Likewise, the **Chinese FIU** does not maintain separate statistics on financial investigations related to cash conversion/ withdrawal, since such investigations are registered as financial investigations into ML-related suspicious transactions.

The comparative Table with tentative data is presented below:

Country	Share of Financial Investigations Related to Cash Conversion and Withdrawal Transactions *
Kazakhstan	80-90%
Turkmenistan	Not registered
Russia	Most
Uzbekistan	13 %

* - tentative assessment

Section 2 Conclusions

The provided information is not sufficient for conducting comparative analysis across the surveyed countries. However, the received responses indicate that risk of use of cash for ML purposes are assessed as high in Russia and Kazakhstan.

In particular, in the Republic of Kazakhstan, cash conversion is a separate type of illegal entrepreneurial activity with involvement of companies that appear to be fake (fictitious) ones. Assets/funds illegally converted into cash may be further integrated into legitimate circulation.

The annual growth rate of criminal offences committed with involvement of fly-by-night companies is 20-30%. Besides that, cash conversion service providers may be utilized for tax evasion purposes as well as for bribing corrupt officials who hold public procurement tenders.

Despite a relatively small number of financial investigations into illegal cash conversion/ withdrawal schemes, the surveyed countries develop and use risk indicators for identifying suspicious cash conversion transactions.

3. ANALYSIS AND CATEGORIZATION OF TYPOLOGIES AND SCHEMES RELATED TO CONVERSION OF CRIMINAL PROCEEDS INTO CASH

3.1 TYPES OF CRIMINAL PROCEEDS GENERATING OFFENCES

Cash withdrawal transactions as such do not constitute a criminal offence, but may be associated with a number of predicate or ML offences.

In the **Republic of Kazakhstan**, the main criminal cash generating offences include: misappropriation or embezzlement of entrusted property (CC Article 189), pseudo-entrepreneurship (CC Articles 215 and 216), fraud (CC Article 190), tax evasion (CC Articles 244 and 245), acceptance of bribe (CC Article 366), obtaining illegal remuneration (CC Article 247 УК), etc.

The 2016 legal statistics provided by Kazakhstan show that **about 85%** of all criminal proceeds in the country are generated through tax and corruption offences.

From the knowledge and experience of the **Russian Federation**, it can be concluded that activities involving illegal cash conversion may be associated with the following criminal offences:

- *Fraud (CC Article 159);*
- *Misappropriation and embezzlement (CC Article 160);*
- *Illegal entrepreneurship (CC Article 171);*
- *Illegal banking activity (CC Article 172);*
- *Forgery or sale of counterfeit payment documents (CC Article 187);*
- *Evading corporate taxes and/or duties (CC Article 199);*
- *Legalization (laundering) of funds or other assets obtained by third parties through crime*

(CC Article 174);

- Legalization (laundering) of funds or other assets obtained by a person through crime (CC Article 174.1).

According to the practical experience of the financial investigation agencies of the State Control Committee of the **Republic of Belarus** the main cash generating offences include tax evasion and unlicensed entrepreneurship.

In **Montenegro**, the main sources of cash represent crimes of unauthorized production and trafficking in narcotic drugs and financial crime offenses with elements of corruption.

In **Turkmenistan**, the main criminal proceeds generating crimes include corruption-related offences, tax offences, large –scale smuggling of goods and embezzlement of entrusted property.

Conclusions:

Analysis of responses provided by the surveyed countries allowed us to compile the list of the most common proceeds generating offences that involve illegal withdrawal of cash:

- **Tax offences;**
- **Corruption-related offences;**
- **Misappropriation and embezzlement of entrusted property;**
- **Illegal entrepreneurship and illegal banking activity;**
- **Fraud.**

Thus, the similar sources of illicit (criminal) financial flows are observed in different countries.

In general, the responses of the surveyed countries correlate with the global trends related to predicate offences. The largest illicit (criminal) flows in the world are generated by tax and corruption-related offences.

It is obvious that, for example, the taxation system contains potential criminal proceeds generating elements which include, in particular, possibility of declaring fictitious expenses.

Likewise, the corruption-related offences involve illegitimate or unsubstantiated allocation and distribution of budgetary funds.

The coordinated efforts of the LEAs, supervisors, tax authorities and FIUs are required for combating illegal cash conversion activities in effective and efficient manner.

3.2 MAIN MECHANISMS AND TOOLS USED FOR INTEGRATING CRIMINAL CASH INTO LEGITIMATE CIRCULATION

From the knowledge and practical experience of the **Republic of Kazakhstan**, it follows that the main mechanisms used for integrating criminal funds into legitimate circulation involve purchase of movable/ immovable property and movement of funds abroad with their subsequent reinvestment back as “clean” money.

From the experience of the **Russian Federation**, it can be concluded that the main mechanisms used for integrating cash obtained through crime into legitimate circulation include:

- purchasing and selling real estate property and transport vehicles;
- purchasing and selling savings certificates and insurance policies;
- granting loans to individuals and legal entities;
- contributing cash to the authorized (statutory) capital of legal entities;
- using cash in casinos and other gambling and entertainment venues;
- other.

In addition to the banking system, non-bank institutions are also engaged in suspicious cash circulation. Due to the specificities of their activities, consumer credit cooperatives and micro-finance organizations are the main sectors used for cash conversion.

The standard scheme of cash conversion through consumer credit cooperatives and micro-finance organizations operates as follows:

Companies (primarily companies that appear to be fake (fictitious) ones) transfer funds to

current accounts of such cooperatives and organizations under interest-bearing loan agreements, after which these funds are further transferred to accounts of natural persons who withdraw them in cash.

In the **Republic of Belarus**, one the methods used for integrating ill-gotten cash into legitimate circulation includes contribution of such criminal cash to the authorized (statutory) capital of business entities or provision of such criminal cash as loans for funding core activities of business entities.

It is noteworthy that the financial investigation agency identified cases where illegally converted cash was used for bribing the corrupt officials.

Conclusions:

Money laundering is aimed at separating criminal proceeds from underlying offences and giving these funds the appearance of having a legal origin. This is the general definition of money laundering that gives insight into this offence.

It follows from the received responses that similar methods are generally used for integrating criminal cash into legitimate circulation:

- acquisition of movable/ immovable property in and outside the country;

- creation of business entities and making contributions to authorized (statutory) capital of legal entities;

- movement of cash abroad followed by reinvestment back as "clean" money

Given that real estate property is exposed to high risk of misuse for money laundering purposes, the countries should consider introduction of a requirement according to which all real estate deeds shall necessarily be notarized, since, at present, many real estate deals are carried out under simple written agreements.

Besides that, transactions involving purchase and sale of saving certificates and insurance policies should also be carried out exclusively through entities that are subject to financial monitoring, and the supervisory authorities should take necessary measures to ensure that these entities comply with the AML/CFT legislation.

3.3 TYPOLOGIES AND SCHEMES OF CONVERSION OF CRIMINAL PROCEEDS INTO CASH

Based on the comparative analysis of the provided schemes and information, we developed a generic typology of flow of funds in the process of their conversion into cash.

After that, we considered the most common typologies of predicate offences and further laundering of obtained criminal proceeds through cash conversion transactions.

Generic Cash Conversion Scheme

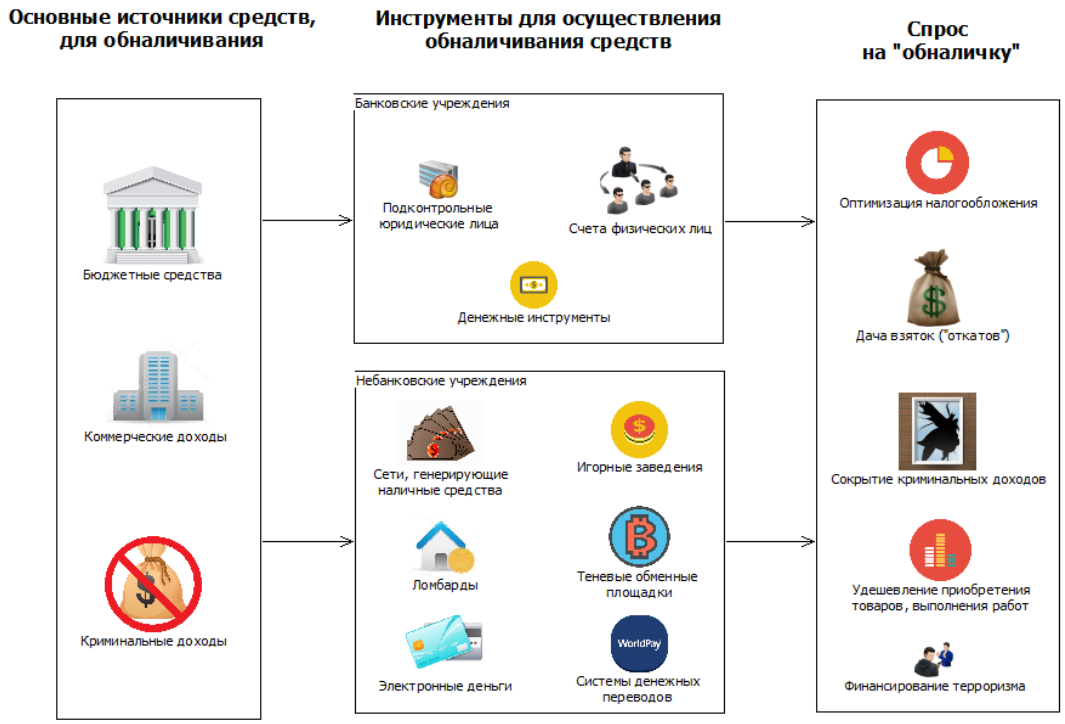
Основные источники средств для обналичивания	**Main sources of funds converted into cash**
Бюджетные средства	Budgetary funds
Коммерческие доходы	Commercial revenues
Криминальные доходы	Criminal proceeds

Инструменты для осуществления обналичивания средств	**Cash conversion instruments**
Банковские учреждения	Banking institutions
Подконтрольные юридические лица	Controlled legal entities
Счета физических лиц	Accounts of natural persons
Денежные инструменты	Monetary instruments

Небанковские учреждения	Non-bank institutions
Сети, генерирующие наличные средства	Cash generating retail networks
Игорные заведения	Gambling venues
Ломбарды	Pawnshops
Теневые обменные площадки	“Shadow” exchange service providers
Электронные деньги	E-money
Системы денежных переводов	Money transfer systems

Спрос на «обналичку»	**Demand for cash conversion services**
Оптимизация налогообложения	Tax optimization
Дача взяток («откатов»)	Bribery (paying kickbacks)
Сокрытие криминальных доходов	Concealment of criminal proceeds
Удешевление приобретения товаров, выполнения работ	Decreasing costs of purchased goods, performed work
Финансирование терроризма	Terrorist financing

Обобщенная схема обналичивания денег



1. Illegal cash conversion and tax offences

1) Use of accounts of fly-by-night companies

Based on the provided materials, information obtained from the LEAs and information from open sources it can be concluded that **fictitious or fake companies** are the most widespread vehicles used for laundering criminal proceeds. Most frequently they are used for committing tax offences and misappropriating the budgetary funds.

Two scenarios of mutual payments made between counterparties and fake (fictitious) companies have been identified:

a) Under the first scenario, funds are transferred to the account of a fake (fictitious) company. After that, these funds are converted into cash and returned to a buyer net of 5-10% commission fee

charged by the fake company for cash conversion and invoicing services. Then, the buyer offsets the VAT on purchased goods (work, services) based on a fake invoice and creates fake deductions to offset actual annual income. Payments for goods (work, services) are made in cash, and the purchased goods (services) are typically of poor quality, since most funds are kept by the taxpayer.

The issued invoice allows the taxpayer to artificially increase expenses (liabilities) of the company and decrease income (assets) indicated in a tax return.

Typical Cash Conversion and Tax Evasion Scheme

Типовая схема обналичивания денежных средств и уклонение от уплаты налогов

Примечание:
Обнальной компанией фактическая реализация товаров (работ, услуг) не осуществлялась.

1 этап	Stage 1
Выписана счёт-фактура	Invoice is issued
Уклонение от уплаты налогов за счет отнесения суммы на вычеты по КНП и в зачёт по НДС согласно полученной счет-фактуре	Tax evasion by artificially decreasing taxable corporate income and offsetting VAT based on the invoice
Компания-получатель	Recipient company
2 этап	Stage 2
Перечисление в банк суммы, указанной в счет-фактуре	Amount indicated in invoice is transferred to bank
Банк	Bank
3 этап	State 3
Обнальная компания снимает наличные с банковского счета	Cash conversion service provider withdraws cash from bank account
Обнальная компания	Cash conversion service provider
Имеющая признаки лжепредпринимательства (отсутствие по адресу, зарегистрированных на «подставное лицо» и т.п.)	Appears to be fake company (no physical presence at registration address; registered in the name of front man; etc.)
4 этап	State 4
Возврат наличных за минусом % за обналичивание денег	Cash is returned net of cash conversion commission fee
Note:	

Cash conversion service provider does not sell any goods (perform any work, provide any services)

b) Under the second scenario, a business entity simply buys a fake invoice from a fly-by-night company. After that, it also offsets the VAT on allegedly purchased goods (services) based on this false invoice and reduces the amount of payable corporate income tax. In this case, no funds are actually transferred to the account of the fly-by-night company.

2) Use of accounts of natural persons

Accounts of natural persons may also be used for committing tax offences.

Funds held on the account of a legal entity are transferred to accounts of natural persons allegedly as remunerations, compensation of travel expenses, official entertaining expenses, etc.

There may be dozens or event hundreds of natural persons involved in the scheme. The scheme operator may use the services of straw men, and cash may be withdrawn from card accounts by third parties (customers) using ATMs.

The legal entity uses these debit transactions for declaring expenses in order to reduce the amount of taxable corporate income tax.

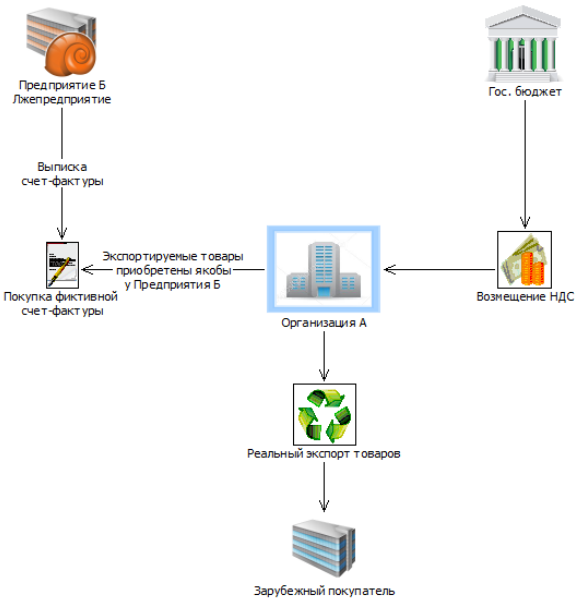
3) Illegal VAT refund

By making and receiving payments to/from complicit fake companies under fictitious sales and purchase contracts, exporters artificially inflate the price paid for purchased goods and, hence overstate the amount of allegedly paid VAT. For making it harder to detect such fraudulent scheme, a long chain of the so-called “transit companies” is used for concealing the fake company, which is the last link in this chain.

After that, exporter actually exports goods abroad, claiming refund of VAT allegedly paid on purchase of the goods from a fake company.

Upon receipt of VAT repayment, these funds are often withdrawn in cash for concealment and further integration into legitimate circulation.

At present, no instances of direct purchase of fake invoices are detected in practice. Instead, a chain composed of 5-10 transit companies is used for making it harder to reveal a fictitious nature of purchase of goods in the territory of a country.



Illegal VAT Refund Scheme

Предприятие Б	Company B

Лжепредприятие	Fake company
Гос. Бюджет	State budget
Выписка счет-фактуры	Invoice is issued
Покупка фиктивной счет-фактуры	Fake invoice is bought
Экспортируемые товары приобретены, якобы, у предприятия Б	Exported goods are allegedly purchased from company B
Организация А	Company A
Возмещение НДС	VAT refund
Реальный экспорт товаров	Actual export of goods
Зарубежный покупатель	Foreign buyer

The following indicators of transactions involving illegal conversion of tax offence proceeds into cash have been identified:

- Company operates for a short period of time (after registration, re-registration);
- Company directors/ founders are straw men who have criminal record, seriously ill persons, drug addicts and mentally disabled persons registered with drug dependence and psycho-neurological clinics;
- Company director is either too young or too old person;
- Financial transactions are inconsistent with a company business profile;
- Cash is regularly withdrawn shortly after funds are credited to account;
- Cash is regularly withdrawn by persons acting under power of attorney;
- Cash withdrawal transactions are carried out during one fiscal period, after which no financial transactions are carried out any more;
- Money is received as remuneration for a broad range of services provided by companies that have no fixed assets and (technical, material) resources;
- Company has small number of staff or no staff at all;
- Transit nature of bank account: incoming funds are withdrawn in cash shortly after they are credited to account;
- A large number of invoices is issued;
- Additional tax returns reflecting new invoices are filed on a regular basis;
- Large volume/value debit transactions are reflected in tax returns, while no funds are actually transferred to contractors/ counterparties;
- Failure to file tax return at the end of a fiscal period;
- Use of registration address where many other companies are registered;
- Company is not physically present at its registration address.

2. Illegal cash conversion schemes associated with corruption-related offences:

1) Use of fake (fictitious) companies for illegal cash conversion to pay kickbacks to corrupt officials

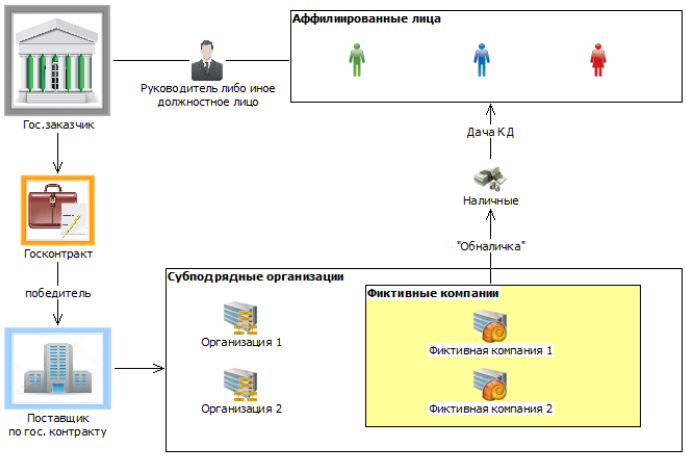
The government authorities transfer funds to the account of a supplier under the public procurement contract. The latter engages subcontractors, including fake companies, to convert the received funds into cash for paying kickbacks (20-30% of contract cost) to the corrupt officials. Such kickbacks are typically paid when advance payments are made to the winners of public procurement tenders.

After that, in order to compensate the incurred costs and make profit, parties to which public procurement contracts are awarded purchase cheaper goods (work, services) in breach of the design specifications and cost estimates, and also use fly-by-night companies for tax evasion purposes.

In case of large public procurement contracts, suppliers typically engage subcontractors, some of which may be utilized for conversion of the received funds into cash, which is further paid as kickbacks.

At the same time, subcontractors may also be used for tax evasion purposes.

In this context, it is important to identify dummy companies that are engaged in the capacity of subcontractors under public procurement contracts.



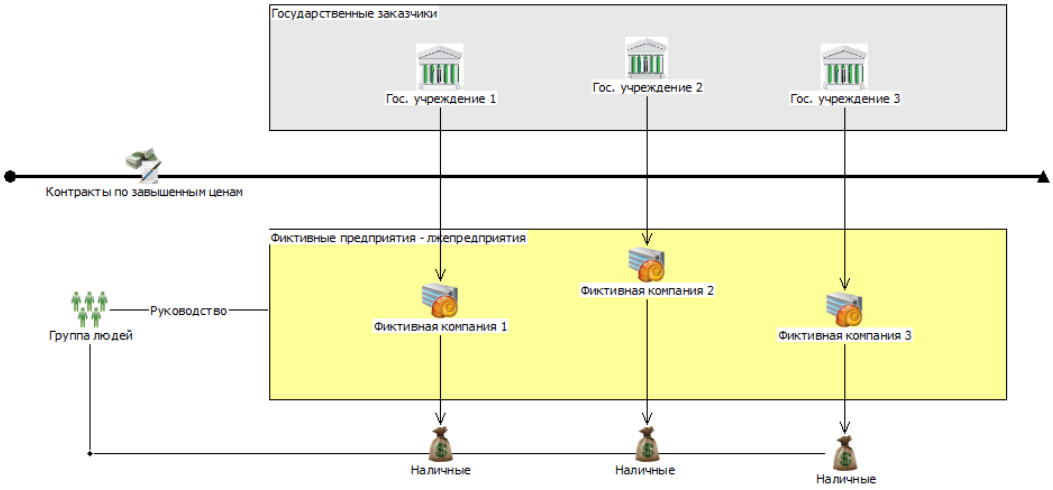
Scheme of Illegal Cash Conversion for Paying Kickback

Гос. Заказчик	Government customer
Руководитель либо иное должностное лицо	Head or other executive officer
Аффилированные лица	Affiliated persons
Госконтракт	Public procurement contract
Победитель	Winner
Поставщик по гос. Контракту	Supplier under public procurement contract
Субподрядные организации	Subcontractors
Организация 1 (2)	Company 1 (2)
Фиктивные организации	Fake companies
Фиктивная компания 1 (2)	Fake company 1 (2)
«Обналичка»	Cash conversion
Наличные	Cash
Дача КД	Bribe (kickback)

2) Embezzlement or misappropriation of budgetary funds

Typically, embezzlement schemes involve overpricing of goods, work and services. For example, a supplier under a public procurement contract signs an agreement with a foreign company for supply of goods at artificially inflated price. When entering into the agreement, the parties agree the mechanism through which the excessive portion of funds will be returned back. Funds paid in excess of the actual cost of goods are typically transferred to accounts of legal entities controlled by executive officers as loans or as remuneration for provision of fake services. In some cases, funds are transferred to debit cards of individuals affiliated with executive officers.

In case of direct misappropriation, budgetary funds are transferred to account of a legal entity, to which a public procurement contract is awarded, after which these funds are instantaneously withdrawn from the account. It is noteworthy that such companies often have nominee directors and founders for concealing identity of true beneficial owners.



Scheme of Misappropriation or Embezzlement of Entrusted Budgetary Assets

Государственные заказчики	Government customers
Гос. учреждение 1 (2, 3)	Government institution 1 (2, 3)
Контракты по завышенным ценам	Overpriced contracts
Фиктивные предприятия – лжепредприятия	Fake companies
Фиктивная компания 1 (2, 3)	Fake company 1 (2, 3)
Руководство	Senior managers
Группа людей	Group of individuals
Наличные	Cash

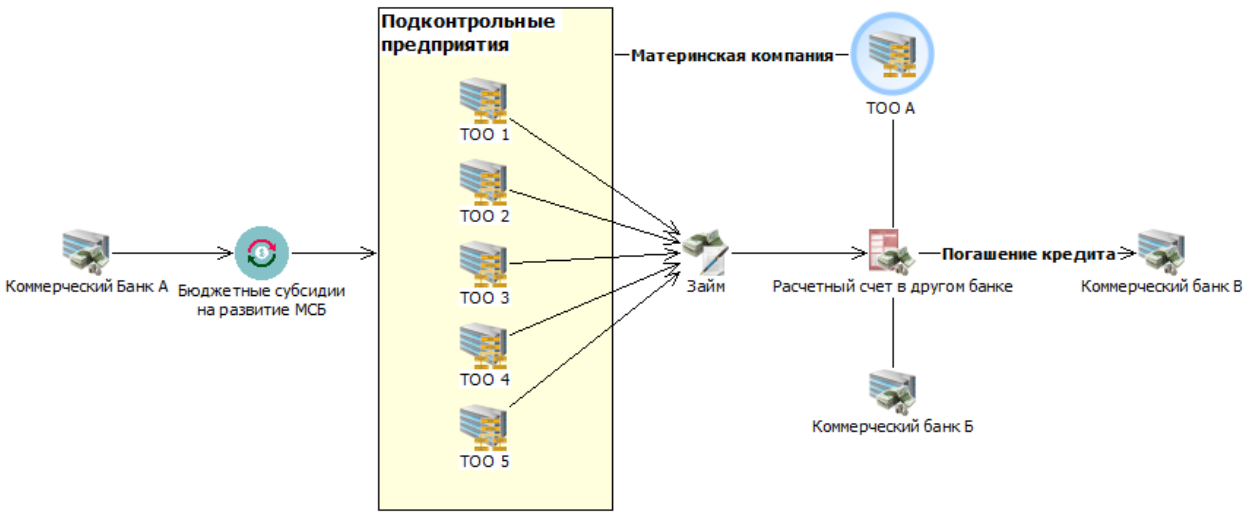
3) Illegal receipt or misuse of government funded loan

The scheme involving illegal receipt or misuse of government funded loan is essentially similar to the schemes described above.

Illiquid real estate property with high assessed value is offered as a security of a loan. Companies prefer to convert received funds into cash or to move them through “shadow” schemes for hiding money from financial monitoring authorities.

For granting unjustified loans, heads of bank branches receive illegal remuneration amounting to several percent of provided loan.

Such actions of senior bank managers constitute criminal offences of commercial bribery and abuse of power.



Scheme of Misuse of Government Funded Loan

Подконтрольные предприятия	Controlled companies
ТОО 1 (2 … 5)	Company 1 (2 … 5)
Материнская компания	Parent company
ТОО А	Company A
Коммерческий банк А	Commercial bank A
Бюджетные субсидии на развитие МСБ	Government funded loan for supporting small and medium businesses
Займ	Loan
Расчетный счет в другом банке	Account in different bank
Погашение кредита	Repayment of loan
Коммерческий банк Б	Commercial bank B

4) Receipt of bribe or abuse of power

In practice, the LEAs encounter multiple cases, where an executive officer or a person entrusted with some functions, acting for his/her personal benefit or for benefit of other persons or organizations, receives funds transferred into accounts opened with bookmakers' offices, electronic payment system operators, or receives direct payments through money transfer system providers. Sometimes, funds are directly transferred to personal accounts of such executive officers or persons affiliated with them.

This type of offences also includes petty corruption.

Further actions of such persons are obvious: transferred funds are typically converted into cash shorty after they are credited to account for separating the funds from originators and disguising their illegal origin.

In case of electronic money, "shadow" cash conversion service providers may be used for these purposes.

Based on the presented case examples and information provided by the LEAs, the following indicators may be used for identifying potential corruption-related offences:

- Public officials and suppliers under public procurement contracts are affiliated with each other;
- Business relationships exist between multiple entities affiliated with public official and multiple entities affiliated with supplier under public procurement contract;
- Public procurement contracts are awarded without holding a tender (the so-called "procurement from one source"), i.e. contract is directly signed with the supplier;
- Large advance payments (20% and more) are made under public procurement contracts;
- Unreasonably short period of time for performance of a public procurement contract;
- Several legal entities affiliated with each other participate in a public procurement tender;
- Suspiciously high price of purchased goods, work and services (potential overpricing);
- Supplier under public procurement contract has no experience in performing the relevant work and/or providing the relevant services;
- Director of a company discharges only "technical" functions; company is actually managed by other persons under power of attorney;
- Suppler under public procurement contract is a newly established company;
- No information on business activity of a supplier in available in open sources;
- Supplier engages dummy (front) companies as subcontractors;
- Contractor or subcontractors do not have sufficient material, human or technical resources for performing their obligations under government procurement contract;
- Significant amount of money received by a supplier under government procurement contract is transferred to accounts of subcontractors;
- Senior managers of banks and loan recipients are affiliated with each other;

- Large loan is granted to company that has no material, human and technical resources, after which received funds are withdrawn in cash or transferred to accounts of other individuals/ legal entities.

3. Criminal offences against property

Property misappropriation may include both misappropriation of entrusted property and illegal receipt of property as a result of unauthorized disposal of entrusted property.

Sources of funds include proceeds obtained through typical criminal offences, such as theft, robbery, extortion racket, petty theft.

Crimes against property (theft, robbery, racket) are aimed at obtaining, in illegal way, highly liquid goods, such as jewelry, computer equipment, motor vehicles, etc.

If property is not subject to mandatory government registration, criminals often use informal "grey" markets for selling stolen property at lower prices.

These markets, in turn, ensure necessary anonymity and prompt conversion of stolen property into cash.

Property obtained through crime may also be sold through pawnshops.

Typical indicators of laundering of assets obtained through commission of the aforementioned criminal offences include:

- Frequent loans received from pawnshops against various types of property used as security;
- The same person regularly takes loans from different pawnshops against a broad range of property used as security;
- Pawnshop operator has a criminal record;
- Contractual price of an item is obviously inconsistent with its actual cost;
- Precious metals, precious stones and jewelry made thereof are sold at prices that differ significantly from the market prices.

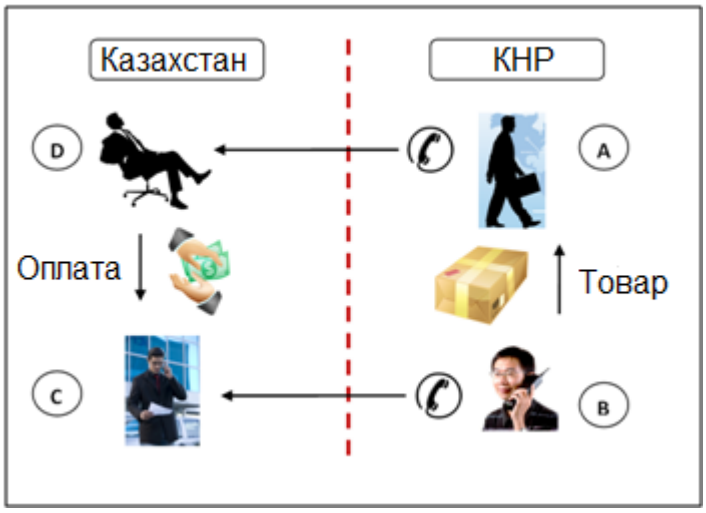
4. Smuggling of goods

Goods are smuggled into a country in order to evade paying customs duties. Payments for such goods are made in cash in order to evade foreign exchange control of export/import operations and reduce goods importation costs.

Goods are sold at wholesale price for cash. Thus, smuggled goods are converted into cash. After that, the received cash is used for paying for the next supply of goods and integrated into legitimate circulation.

Bank wire transfers, money transfers without opening bank accounts, cash couriers and informal hawala-type money transfer systems may be used for payment for supply of goods.

Case example: *A Kazakh citizen (individual A) travels to China. He decides to buy goods for further sale and needs money to pay for goods. A Chinese seller in China (individual B) has the friend in Kazakhstan (individual C who is the Chinese businessman staying in Kazakhstan). The Chinese seller in China (individual B) recommends the individual A to hand over money for goods to the individual C in Kazakhstan. The individual A calls his friend or relative (individual D) in Kazakhstan and requests him/her to pay money to the individual C. After the individual C receives money in Kazakhstan, the individual B hands over goods to the individual A in China. The individuals D and/or C may use bank accounts for making the settlement. In this scheme, the Chinese entrepreneur provides informal payment services that help the Kazakh entrepreneur to buy goods without any formal documentation.*



Payment Scheme Used for Informal Trade

Казахстан	Kazakhstan
КНР	China
Оплата	Payment
Товар	Goods

Operation of hawala-type systems (in particular, in Kazakhstan) is featured by the following main specificities:

- They are most frequently used for payment for informally imported goods;
- They accept new customers only upon recommendations of persons well known to them;
- Amount of commission charged by them for their services is lower compared to fees charged by official money transfer providers, especially when money is sent to countries other than the CIS member countries;
- They do not carry out transactions involving small amounts of money (e.g. less than USD 10 thousand).

These channels are obviously vulnerable to ML/TF, since offenders may prefer to use the advantages of these "underground" informal money transfer systems.

Based on the examined materials, the following typical indicators have been identified:

- Regular cross-border money transfers with and without opening bank accounts to recipients located in a particular country;
- Amounts of regular cross-border money transfers are below the threshold set forth in the financial monitoring legislation and foreign exchange control regulations;
- Regular cross-border transportation (in both directions) of cash by one person or by a group of persons;
- Regular payments in foreign currency and foreign currency transfer transactions without presentation of contracts/ agreements according to which payments should be made in foreign currency;
- Regular foreign currency exchange transactions in border zones;
- Frequent use of torn or dirty bank notes in cross-border transactions.

5. Fraud and pyramid schemes

Fraud offences include widespread pyramid schemes and various financial scams.

1) Financial pyramids are most frequently disguised as investment funds offering profit-making opportunities to their participants. For giving the appearance of legitimacy, websites are created on which formal individual accounts of "investors" are maintained.

"Investments" may be made both in cash through the authorized agents and in cashless form through bank accounts, payment systems and e-money systems.

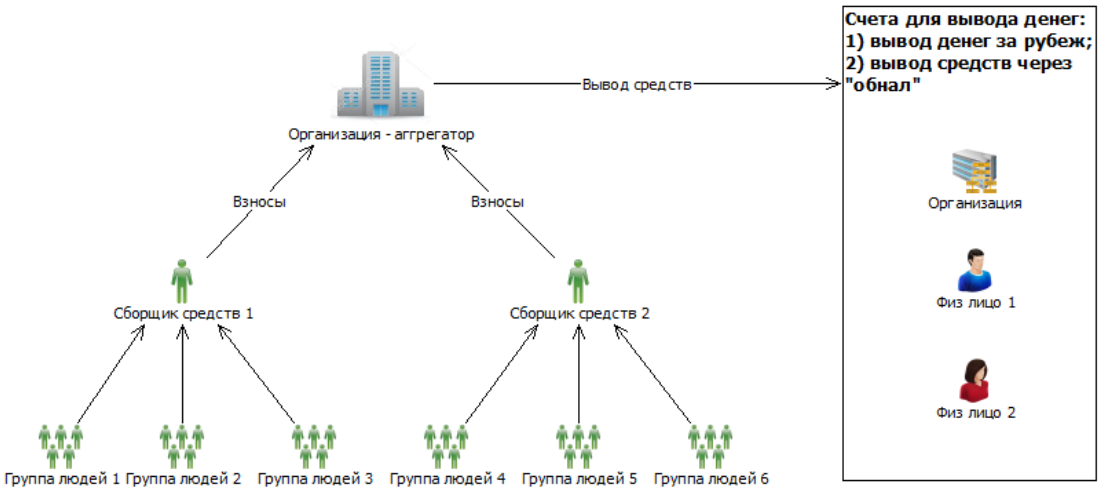
Over a certain period of time, all funds are accumulated on commingled (pooled) accounts of a financial pyramid, after which these funds are wire transferred to "transit companies" and are further moved abroad or converted into cash.

2) Fraud schemes

Fraud schemes may involve fake online stores and scam shopping websites designed such as to look like well-known online shopping sites, on which various fraudulent advertisements are posted.

E-wallets are used as means of payments for non-existent goods. In order to remove account limitations, fraudsters use the "account identification" services. For this purpose they typically use personal data of nominal account holders (straw men).

After funds are credited to account, fraudsters move them from the e-money system by transferring them to bank card accounts or by sending them via money transfer systems.



Scheme of Conversion of Financial Pyramid Proceeds into Cash

Организация – агрегатор	Aggregator
Взносы	Investments
Сборщик средств 1 (2)	Funds collector 1 (2)
Группа людей 1 (2 … 6)	Group of persons 1 (2 … 6)
Вывод средств	Movement of funds
Счета для вывода денег:	Accounts for moving funds
1) вывод денег за рубеж;	1) Funds are transferred abroad
2) вывод средств через «обнал»	2) Funds are withdrawn in cash
Организация	Business entity
Физ. лицо 1 (2)	Natural person 1 (2)

Indicators of potential financial pyramid and fraud scheme may include the following:

- Multiple transfers or deposits of funds into account by various natural persons followed by withdrawal of funds in cash or their transfer to other accounts;
- Absence of permits (licenses) to accept deposits from general public;
- Natural persons transfer/ deposit funds as financial aid or non-remunerable contributions;
- Natural person is apparently not involved in any business activities: has not created individual entrepreneurship; has no share/ interest in authorized capital of legal entities;
- Funds are raised without any formal loan agreements;

- Transactions are inconsistent with company business profile;
- Use of dummy articles of incorporation/ association;
- Deposit interest rate is significantly higher than official refinance rate;
- Deposits and transfers are made within a short period of time after account of a legal/ natural persons is opened;
- Information from open sources suggests fraudulent activities (financial pyramid scam);
- Legal entity is not involved in any business activities: has no staff, fixed assets, corporate counterparts, etc.;
- Transit nature of commingles (pooled) account on which funds are accumulated;
- Complex chain of transactions carried out after receipt of funds.

5. Cybercrime and unauthorized access

Cybercrimes committed for stealing/ misappropriating property deserve increased attention in the context of money laundering, since criminals who commit these offences derive financial or other material benefit in form of illegal proceeds. The primary goal of criminals is to get access to bank databases and customers' card accounts. For this purpose offenders use modern software and hardware systems and apply social engineering techniques.

Cybercrimes may be generally divided into two categories:

1) Theft of payment card information and ATM fraud;

2) Unauthorized access to account management systems.

Criminals traditionally use plastic card skimming and cloning methods for stealing payment card information.

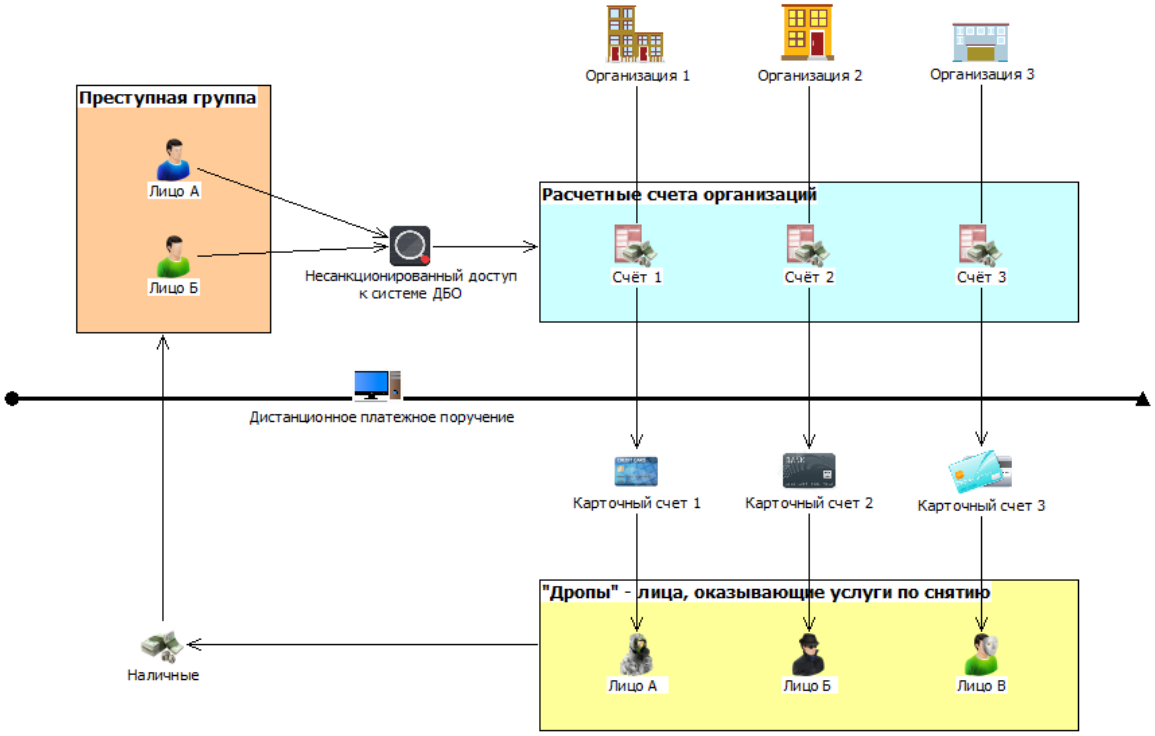
Besides that, remote banking services (online banking) are also exposed to high risk.

The main targets of attacks on online banking are files of victims with digital/ electronic signatures which allow offenders to obtain access to individual and corporate accounts.

After obtaining remote (online) access, offenders transfer funds to designated individual or corporate accounts, after which these funds are withdrawn or otherwise converted into cash.

Where criminal proceeds are obtained as a result of theft of funds held on bank accounts, criminals use banking transactions for laundering these ill-gotten proceeds.

Организация 1 (2, 3)	Entity 1 (2, 3)
Преступная группа	Criminal group
Лицо А (Б)	Person A (B)
Несанкционированный доступ к системе ДБО	Unauthorized access to online banking
Расчётные счета организаций	Entities' accounts
Счет 1 (2, 3)	Account 1 (2, 3)
Дистанционное платежное поручение	Online payment instruction
Карточный счет 1 (2, 3)	Card account 1 (2, 3)
«Дропы» - лица, оказывающие услуги по снятию	Money drops – individuals used for withdrawing cash
Лицо А (Б, В)	Person A (B, C)
Наличные	Cash



Scheme of Conversion of Proceeds Obtained through Unauthorized Access to Online Banking into Cash

Bank accounts opened in advance in the name of nominee holders are used for laundering criminal proceeds. Such accounts are opened with the same bank to expedite transfer of stolen funds. After stolen funds are successfully transferred, offenders seek to convert them into cash within the shortest possible period of time.

International transfers are used less often, since in this case additional efforts are required: offenders have to convert stolen funds into foreign currency; provide contract (under which payments in foreign currency are made) for foreign exchange control purposes; and find and prepare a foreign, *inter alia*, offshore company.

The main indicators of laundering proceeds obtained through cybercrimes include:

- Multiple debit transactions (money transfers) from different card accounts to other card account(s), including foreign accounts;
- Regular transactions with the use of card accounts via one or several payment terminals;
- Use of fake (transit) companies with subsequent withdrawal of cash or transfer of funds abroad;
- Director is unaware of business profile of company headed by him/her;
- Chain of transactions carried out remotely (online) through multiple accounts;
- Involvement of large number of foreign nationals and legal entities;
- Absence of apparent business relationships among parties to transactions;
- Transactions are carried out in evening or at night;
- Use of large number of money drops (individuals used for withdrawing cash);
- Withdrawal of cash from ATMs by persons who try to disguise themselves (wearing sunglasses, hats that cover their faces, etc.);
- Consecutive cash withdrawals by the same person from ATMs located nearby each other;
- Funds are transferred to a large number of natural persons who withdraw them in cash;
- Natural persons cash out received funds from accounts in evening or at night;
- Funds are converted into e-money through exchange sites;

- Use of foreign IP addresses;
- Frequent change of IP addresses.

6. Proceeds from distributions of narcotic drugs and other prohibited substances

In practice, various methods are used for paying for narcotic substances: direct cash payments; exchange for other liquid assets; wire transfers to bank accounts; transfers via money transfer systems; and/or transfers/ deposits to e-wallet accounts. The latter have become the most widespread instruments used in recent years.

E-wallets provide a number of advantages necessary for further laundering of criminal proceeds.

Typically, criminals devise the schemes of distribution of drugs and other banned substances in advance. The schemes involve several layers of the so called “grey”, “semi-grey” and “white” e-wallets.

Scheme of Flow of Criminal Proceeds with Use of E-Money and Exchange Sites

Источник	Source
Серый кошелек	Grey e-wallet
Обменник	Exchange site
Полу-белый кошелек	Semi-white e-wallet
Белый кошелек	White e-wallet

Schemes may additionally involve purchase of crypto currencies via exchange sites, making bets in bookmakers’ offices and on online gambling sites and use of liquid digital goods as additional intermediate stages of the layering and conversion process.

In order to conduct successful financial investigations, FIUs should be able to detect “shadow” exchange sites. Accounts opened on such sites are used as transit points in conversion process. The main indicators of such exchange sites include the following:

- Large number of incoming transfers from unidentified “grey” accounts;
- Outgoing transfers to a large number of different e-wallets;
- Many active e-wallets are registered in the name of one person;
- Accounts are managed from one or several static IP addresses;
- Absence of business activities: no goods, services, tickets and other assets are purchased;
- Absence of registration in capacity of official exchange site.

The main indicators of potential laundering of proceeds from illegal distribution of drug substances include:

- Rounded-off amounts of money transfers;
- Funds are further transferred shortly after they are credited to account;
- Same (or similar) payment purposes are frequently stated, where no information is available on professional activities of money recipient;
- And conversely, different payment purposes are stated when payments are made for a

wide variety of services;

- Upon receipt of funds, they are further transferred to accounts of informal exchange sites, bookmakers' offices and online gambling websites;
- Use of anonymous (unidentified) pooled e-wallet accounts – the so-called "grey" e-wallets;
- Funds are not transferred directly to the so-called "white" e-wallets – e-wallets which holders have been fully identified as bona bide customers;
- Use of foreign static IP address for transferring funds to individual accounts having local IP addresses;
- Active use of several "grey" e-wallets from on foreign IP address;
- Regular transfers of e-money to accounts of crypto currency exchange sites.
- Most incoming payments are made in cash via payment terminals.

3.4 INDICATORS THAT CAN BE USED IN AUTOMATED SYSTEMS FOR IDENTIFYING ILLEGAL CASH CONVERSION TRANSACTIONS

#	Subjects	Indicators	Used Databases (DB)
1	Fake (fictitious) companies	*Fake companies are primarily used for committing tax and corruption-related offences in order to withdraw/ transfer criminal proceeds.* - Company is not involved in any actual business activities; - Company operates for a short period of time (less than 1 year) after registration (re-registration); - Company directors and founders have criminal record; - Company directors and founders are either too young or too old persons; - Company directors and founders are drug addicts and/or mentally disabled persons registered with drug dependence and psycho-neurological clinics or are seriously ill; - Company is registered at address where many other companies are registered; - Bank account is opened shortly before transactions are carried out through such account; - Company has few (3 or less) or no employees at all; - Transactions are carried out through account only during one or two fiscal periods; - Multiple large amount invoices issued within on fiscal period; - Person who carries out transactions acts under power of attorney or is accompanied (instructed) by third parties; - Transit nature of bank account: funds transferred to account are withdrawn in cash within a short period of time; - Company is not physically present at its registration address; - Company has no fixed assets (movable and/or immovable property).	DB of financial transactions; DB of registered taxable entities; DB of tax returns; DB of invoices; DB of criminal records; DB of movable property; DB of immovable property; DB of persons registered with drug dependence and psycho-neurological clinics.
2	Dummy companies	*Unlike fake (fictitious) companies, dummy companies, in most cases, conduct actual business (economic and financial) activities, but their founders and directors are not actually involved in management of these companies.*	DB of financial transactions; DB of registered taxable entities; DB of tax returns; DB of invoices;

		- Company had or still has material, technical and human resources; - Directors and founders of company are replaced shortly before it becomes engaged in performing public procurement contract(s); - Business operations and activities are fully managed by third parties; - Powers of attorney are issued to third parties for carrying out any types of transactions on behalf of company director; - Significant changes in business activities of company after its government re-registration; - Company director lacks skills, knowledge and experience needed for business success; - Company receives large amount of funds from different budgetary sources after its government re-registration; - Large business entity appears among company founders; - Company address and telephone numbers are the same as those of a large business entity.	DB of criminal records; DB of movable property; DB of immovable property; DB of public procurement contracts; DB of licenses and permits.
3	Fake borrower	*Company that is created or engaged for illegal (fraudulent) receipt or misuse of granted loans.* - Large single-tranche loan is issued; - Company has no fixed assets (material and technical resources); - Company has few (not more than 3) or no employees at all; - Loan is secured by guarantees of a third company; - Value of assets used as loan security is significantly overestimated; - Borrower's account is virtually inactive (no large regular transactions carried out through account); - Upon receipt of loan tranches, funds are withdrawn in cash; - Upon receipt of loan tranches, funds are transferred to accounts of third entities (persons) that are appear to be fake (fictitious) companies (item 1); - Borrower transfers borrowed funds to offshore companies; - Parent company of borrower has a current	DB of financial transactions; DB of movable property; DB of immovable property.

		loan agreement in force; - Company is appears to be affiliated with bank senior manager(s).	
4	Cash generating entities	*Cash generating entities are companies that have large amounts of cash proceeds from the sales. These may include large consumer goods retail companies, petrol station networks, construction materials retail network, etc., which pose high cash conversion risks.* - Significant decrease in amount of cash proceeds (from sale) collected and deposited into bank account along with increase in amount cashless funds transferred to account; - Significant decrease in amount of cash proceeds (from sale) collected and deposited into bank account by a financially stable company; - Filing additional tax returns for previous (earlier) periods with declaration of additional invoices.	DB of financial transactions; DB of tax returns.
5	Money drops	*Money drops are natural persons who provide services involving withdrawal of cash from card and current accounts and provide payment instruments with identification data and authorization codes for disposal of money held on cards. Money drops also receive funds transferred via money transfer systems and hand over received cash to customers net of commission fee.* - Frequent withdrawals of cash in evening by persons who try to disguise themselves (wearing sunglasses, hats that cover their faces, etc.); - Consecutive cash withdrawals by the same person from ATMs located nearby each other; - Unjustified consecutive cash withdrawals from ATMs, where it is easier to do it in bank; - The same person frequently receives funds send via money transfer systems; - Multiple transfers of funds to account of the same natural person with different payment purposes stated, where no information is available on professional	DB of bank internal information; DB of financial transactions.

		activities of the recipient; - Transfers of large amounts of funds to account of a natural person, where no information is available on his/her professional activities; - Funds are transferred to a large number of natural persons who withdraw them in cash.	
6	"Grey" e-wallets	*"Grey" e-wallets are used for receiving/ collecting funds obtained through crime. After that, such criminal proceeds go through several-stage laundering process for disguising their criminal origin and are further integrated into legitimate circulation.* *"Grey" e-wallets may be used for receiving proceeds from sale of narcotic drugs and other forbidden substances, petty corruption proceeds and other criminal proceeds. "Grey" e-wallets may also be used for terrorist financing purposes.* - Amount of carried out transactions is equal to the maximum threshold established for non-identified e-wallet holders; - E-wallet holder is nominee holder; - Frequent incoming money transfers to a person who is apparently not involved in any business (entrepreneurship) activities; - Different payment purposes are stated; - E-wallet account is replenished primarily by cash deposited via payment terminals; - Use of foreign static IP addresses; - Constant use of foreign IP addresses; - Funds are transferred from e-wallet to e-money account that appears to be exchange site; - No direct transfers involving withdrawal/ movement of funds from the e-money system (to bank accounts, via money transfer systems).	DB of financial transactions; DB of entities that are subject to financial monitoring. Since transaction amounts may reach threshold values established by the AML/CFT legislation, analysis of the listed indicators may be performed by internal control units of reporting entities.
7	"Shadow" exchange sites	*"Shadow" exchange sites provide services involving exchange of various monetary instruments. Such 'shadow" exchange sites often do not apply CDD measures, which increases risk of their misuse for ML/TF purposes.* - Exchange site is not registered as official exchange site;	DB of financial transactions; DB of entities that are subject to financial monitoring. Since transaction amounts may reach threshold values established by the

		- Large number of incoming transfers from unidentified accounts; - Outgoing transfers to a large number of different e-wallets; - Many active e-wallets are registered in the name of one person; - Accounts are managed from one or several static IP addresses; - Absence of business activities: no goods, services, tickets and other assets are traded on account.	AML/CFT legislation, analysis of the listed indicators may be performed by internal control units of reporting entities.
8	Fictitious (fake) bets in bookmakers' offices and gambling venues	*The primary goal of fictitious betting is to return funds with minimum losses. The internal control rules of bookmakers' offices and gambling venues often impose limitations on amount of funds (cash) that can be withdrawn without use of gambling (betting) account. In this context, criminals place the so-called "arbitrage bets" or "miracle bets" that guarantee return of total bets amount (in other words "surebets").* - Player regularly places bets without seeking to win maximum prize (i.e. amount of won money commensurate with amount of money originally held in account); - Player regularly withdraws money after making a "surebet"; - Funds are regularly transferred to gambling account from different accounts; - Player places bets from different countries (different IP addresses); - Several players make bets from the same IP address; - Players use the "intentionally losing" tactics, i.e. money goes in full to a certain player; - One player has several gambling accounts; - Players regularly deposit large amounts of funds into their gambling accounts; - Regular placement of one-time bets followed by withdrawal of money from gambling account; - Won money is transferred to account of other person; - Different players use the same IP address.	DB of financial transactions; DB of entities that are subject to financial monitoring.

3.5 EXAMPLES OF SUCCESSFUL INVESTIGATIONS INTO ILLEGAL CASH CONVERSION CASES

Republic of Kazakhstan

Case example 1: Tax and corruption-related offences. In December 2015, the Almaty Office of the National Anti-Corruption Service disrupted the activities of the organized criminal group led by individuals P and O, who, driven by greed, created and operated fake companies "KS", "IR", "MS" and "AKS" in Almaty city since November 2014 through December 2015, which illegal activity inflicted exceptionally large financial losses on the state amounting to KZT 1.59 billion.

The investigation revealed that the aforementioned individuals engaged other persons in the activities of the criminal group organized by them and assigned individual roles to each of these persons. Besides that, Mrs. V, who was the head of the internal investigation unit of the Almaty Office of the Public Revenue Department, helped to conceal traces of the criminal activity by way of illegal reorganization and acquisition of the fake companies by newly established fake companies registered in the names of straw men, and received illegal remuneration for these services from the members of the criminal group.

Total losses inflicted on the state as a result of unpaid taxes amounted to KZT 2.43 billion, of which KZT 635.1 million were voluntarily returned to the state budget by the business counterparties of these fake companied after they received the relevant notices form the tax authorities, and another KZT 409.9 million were recovered through seizure of the movable and immovable property of the suspects.

The suspects were accused of committing a total of 14 criminal offences (three offences penalized by CC Article 366(3)(2-3); three offences covered by CC Article 367(4); four offences punishable under CC Article 215(3); two offences criminalized by CC Article 245(3); one offence penalized by CC Article 262(1); and one offence punishable under CC Article 262(3), and the case files were submitted to the court for prosecuting the defendants.

At present, this criminal case is considered by the Special Inter-District Criminal Court of Almaty city.

Case examples 2: Misappropriation of budgetary funds. The LEAs instituted 33 criminal cases (under Articles 189(4)(2); 189(3)(2); 190(3)(3.2); 361(2); 215 (2)(2-3); and 369(2) of the RK Criminal Code) against the director of the regional health resort Mrs. M and her husband Mr. K. In 2011-2015, the suspects, acting in conspiracy with the complicit employees of the resort, regularly falsified the records by overstating the number of patients staying at the resort, and, thus, misappropriated KZT47.5 million allocated from the government budget for feeding and medical treatment of the patients.

The director Mrs. M, who sponsored the fake companies "E" and "G" created by her husband, transferred KZT 47.5 million misappropriated by her from the government budget to the accounts of these fake companies.

For laundering the misappropriated budgetary funds allocated for treating patients and paying wages to the resort personnel, in 2013-2015, the director Mrs. M and her husband Mr. K used the stolen funds, that were converted into cash through the aforementioned fake companies, for constructing the 433.3m^2 personal residential house that cost them KZT 36.2 million, and also bought the KZT 6.2million worth car in 2013.

On October 18, 2016, the court founded the director Mrs. M guilty of misappropriation or embezzlement of entrusted property and sentenced her to 7 years of imprisonment with confiscation of property.

Republic of Uzbekistan

Case example 1: Misappropriation of assets. Individual C, being the part-time employee of company "B", conspired with the director and chief accountant of this company for misappropriating assets of other person by way of deception and abuse of trust. The individual C persuaded the individual B, who was the acquaintance of him, to transfer money from the account of his company "K" to the account of company "B" as a loan and promised to repay the loan in one month. The individual B agreed and transferred large amount of funds from the account of company "K" to the account of company "B" allegedly for purchasing mineral fertilizers. After that, in order to convert the received money into cash, the perpetrators transferred these funds to the account of Azot company as payments for mineral fertilizers and sold the fertilizers for cash in the markets located in Fergana Valley.

Thus, the investigation revealed the scheme used for converting the misappropriated assets into cash.

Case example 2: Misappropriation of assets. The analysis of activities of company "M" revealed that this company operated without license and breached the requirements set forth in Uzbek Cabinet of Ministers' Resolution No.306 on "Additional measures to improve the use of cash register machines with fiscal memory" dated November 17, 2011; Resolution No.280 on "Measures to further reduce non-bank money turnover" dated August 5, 2002; and Resolution No.407 on "Measures to streamline registration of and trade by legal and natural persons" dated November 26, 2002.

Further financial investigation revealed that company sold goods for cash in the process of unlicensed operation.

After that, the request was filed with the National Oversight Agencies Coordination Council for conducting unscheduled audit of business and financial operations of company M to verify its compliance with the tax legislation.

The audit confirmed that company M operated without license, did not deposit large amount of cash from sales of goods into the bank account and evaded paying taxes to the national budget.

Republic of Tajikistan

Case example: Corruption-related offence. The Tajik LEAs instituted the criminal case under Article 245(4)(b) (misappropriation and embezzlement at exceptionally large scale), Article 340(2)(a) (repeated forgery of documents) and Article 320(2) (giving bribe to official in exchange for committing knowingly illegal actions) of the Criminal Code against the foreign national A.

It was established in the course of investigation that the suspect A, being the director of the construction company, misappropriated and embezzled over TJS 14 million budgetary funds in the process of construction of facilities funded by the government. In order to conceal the misappropriation of funds, the suspect A offered TJS 3 million as a bribe to the official who conducted the audit of financial activities of the construction company.

As a result of the criminal intelligence and detective operation the suspect A was detained at the moment when he handed over TJS 3 million to the official.

Russian Federation

Presented below are the examples of use of cash of unknown origin, information of which was obtained in course of financial investigations:

Case example 1: The investigation was conducted into activities of the cash courier who presented the bill to the issuing bank for payment. This bill was earlier issued by the bank and was handed over to the suspect through a chain of legal entities. The bank paid the bill by transferring funds to the company that was located abroad and controlled by the suspect. After that, the suspects converted the transferred funds into cash in the territory of the foreign country and brought cash back into Russia;

Case example 2: The investigation in respect of a number of individuals revealed the

operation of several groups composed of the citizens of different countries who bought foreign currency from credit institutions in exchange for large amounts of money of unknown origin. After that, they moved foreign currency abroad, where it was transferred, through financial companies, to the accounts of companies controlled by the suspects (these accounts were opened primarily with foreign banks). The suspects also carried out foreign exchange transactions and brought the purchased currency cash back into Russia;

Case example 3: One of the members of the illegal cash conversion and withdrawal scheme received funds on his bank card account transferred by the controlled legal entities under the loan agreements. After that, he withdrew a portion of the received funds in cash using the ATMs, and used the remaining portion for buying tokens in casinos, which he further exchanged for cash at the casino cash-desk.

Republic of Belarus

Case example 1: Corruption-related offences. In November 2015, based on the results of analysis of suspicious financial transactions conducted by the Financial Monitoring Department (FIU) of the Belarusian State Control Committee the criminal case was instituted against the general director of one of the Belarusian factories who was accused of abusing his power or official position. Acting in conspiracy with the Israeli citizen and using unnecessary intermediary schemes, the director purchased expensive equipment for the factory at a price that was almost two times higher than the actual cost of the equipment which was procured under the investment project funded from the loan provided by the Eurasian Development Bank against the guarantee of the Belarusian Government.

These actions of the director significantly deteriorated the financial standing of the factory and entailed financial losses in amount of EURO 980.5 thousand. These funds misappropriated through the overpricing scheme were transferred to the account of the company registered in the UK and controlled by the Israeli citizen.

After that, in order to give appearance of legitimacy of ownership, possession and disposal of these funds and to conceal and disguise their origin, the perpetrators conducted various financial transactions for transferring the funds from the account of the controlled foreign company to their personal accounts in Belarus and used them for private business, *inter alia*, for payment for the real estate property and the land plot.

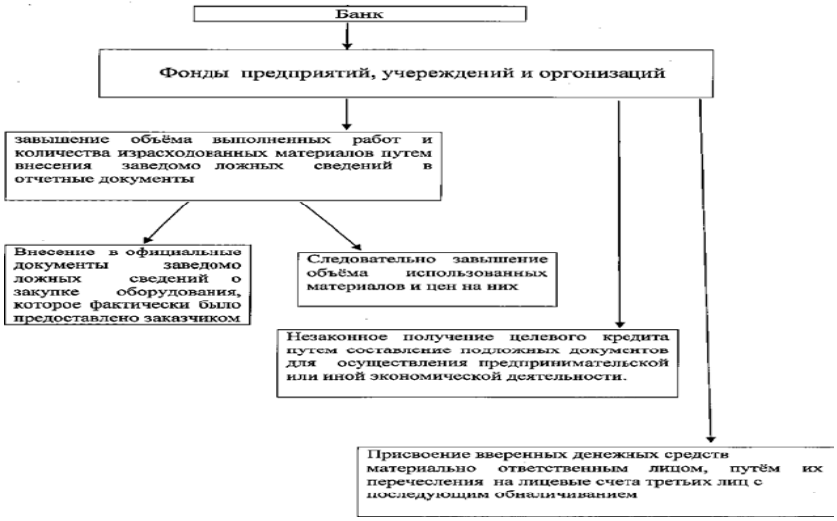
Case example 2: Fraud. In January 2014, the criminal case under Article 209(4) of the Criminal Code was instituted against the directors of two commercial companies and the former officers of the Belarusian tax authorities, who forged the accounting documents and used them for receiving illegal VAT refunds in exceptionally large amount (around USD 347.5 thousand) in May – September 2013. A portion of these funds obtained through fraud was converted into cash through the pseudo-entrepreneurial entities.

Case example 3: Tax offences. In February 2015, based on the intelligence provided by the FIU, the special operation was conducted to disrupt the activities of the organized group. This group had no intention to conduct any legitimate business activities, but instead registered legal entities for concealing and artificially reducing income and other taxable revenues and also used the accounts and addresses of a least 30 controlled pseudo-entrepreneurial entities, including non-resident entities, for assisting executive officers of business entities to evade taxes and launder assets obtained through crime. Criminal cases were instituted against some executive officers of business entities operating in the real sector of economy, who used the services of these pseudo-entrepreneurial entities. These executive officers were accused of tax evasion.

Searches conducted that the inquiry stage resulted in seizure of cash in amount of USD 149 thousand and Euro 7.25 thousand.

Turkmenistan

Case example: Scheme of flow of funds obtained through misappropriation or embezzlement of entrusted property



Банк	Bank
Фонды предприятий, учреждений и организаций	Funds of business entities, institutions and organizations
Завышение объёма выполненных работ и количества израсходованных материалов путём внесения заведомо ложных сведений в отчётные документы	Overstatement of scope of work performed and quantity of materials used by deliberate misrepresentation in reporting documents
Внесение в официальные документы заведомо ложных сведений о закупке оборудования, которые фактически было предоставлено заказчиком	Inclusion, in the official documents, of deliberate misrepresentations about purchased equipment, which was actually provided by the customer free of charge
Следовательно, завышение объема использованных материалов и цен на них	Overstatement of quantity of used materials and their prices
Незаконное получение целевого кредита путем составления подложных документов для осуществления предпринимательской или иной экономической деятельности	Illegally obtaining of a special-purpose loan by falsifying documents related to entrepreneurial or other business activity
Присвоение вверенных денежных средств ответственным лицом, путём их перечисления на лицевые счета третьих лиц с последующим обналичиванием	Misappropriation of entrusted funds by an executive officer by way of transferring these funds to personal accounts of third parties and converting them into cash

3.6 SUSPICIOUS CASH CONVERSION TRANSACTION CRITERIA

Based on the responses provided by the surveyed countries, the following indicators of suspicious cash conversion transactions as well as similarities and differences between them have been identified.

Country	Suspicion Indicators
Similar indicators: Kazakhstan, Russia, Uzbekistan, Belarus, Poland	- Cash is regularly withdrawn from account shortly after funds are credited to the account; - Unusually large amounts of cash withdrawn from an account are inconsistent with the normal account activity; - Regular incoming money transfers made without opening bank accounts, *inter alia*, with the use of electronic means of payment; - Increase in share of cash deposited into individual and corporate accounts followed by withdrawal of money; - Withdrawal of cash from an account that has been dormant for over three (six) months;
Kazakhstan	- Unkempt appearance of a person who regularly withdraws cash from a bank account; - Opening several accounts under the threshold amount with subsequent withdrawal of cash.
Russia	- An individual recipient regularly receives money transfers from a large number of other individuals who make such transfers without opening bank accounts (*inter alia*, with the use of electronic means of payment) and withdraws the incoming funds in cash; - Large amounts of funds are (regularly) credited to the deposit account(s) of individual from other account(s) opened for such individual in different credit institution(s) with subsequent withdrawal of the credited funds in cash;
Uzbekistan	- Cash deposits by an individual in amount equal to or exceeding 500-fold minimum wages at the day of transaction into the bank account of a legal entity or an individual entrepreneur as a loan, financial assistance and/or contribution to the authorized (statutory) capital; - Transactions (payments or cash withdrawals) carried out with the use of five or more international payment cards during one day via a terminal of the same operator, where amount of transactions performed with the use of each card is equal to or exceeds 25-fold minimum wages; - One-off or multiple sales or purchases by individuals of foreign currency cash in amount equal to or exceeding 500-fold minimum wages during a period not exceeding 3 months;
Belarus	- Acceptance of collectable foreign currency cash and/or payment documents denominated in foreign currency which are suspiciously dirty; - One-off or multiple deposits (during the reviewed period) of cash for acquisition of property, where information on the depositor available to the financial institution does not allow it to determine the origin of the deposited cash; - One-off or multiple deposits/ withdrawals (during the reviewed period) of cash into/from an account (except for deposits/ withdrawals of cash by individuals to/from bank deposit account(s)), where the available information on the party to such transactions does not allow for determining the origin of this cash; - One-off or multiple purchases/ sales (during the reviewed period) of foreign currency cash, where the available information on the party to such transactions does not allow for determining the origin of the cash; - Inheritance of cash, precious metals and items made thereof included in the list of heritable items, where there are no documents certifying their ownership by a party who has bequeathed such items; - Similar financial transactions carried out by a representative on behalf of three and more parties, if such transactions involve deposits or withdrawals of cash or highly liquid financial instruments; - Payments for purchased immovable (movable) property are made in cash.
Poland	- Person paying or withdrawing cash is accompanied by third persons; - Person paying of withdrawing cash refuses to provide personal data; - Look and behavior (such as ability to make a disposal) of person paying or withdrawing cash suggest that he or she cannot own paid money;

	- Undefined or vague titles of payments.

CONCLUSION

Illegal cash conversion remains one of the urgent problems faced by the surveyed countries.

FIUs, Central Banks, tax authorities and law enforcement agencies realize the urgent need to eradicate the root causes and conditions that facilitate existence and outspread of this phenomenon.

The efforts undertaken by the governments for eliminating illegal cash conversion activities are basically pursued at two levels: at the national level – through improvement of the relevant legislation; and on the tactical level – by regular identification and disruption of such illegal schemes.

The countries may consider the following conclusions as proposals for improvement of the national legislation.

1. Improvement of tax legislation

Since tax offences are widespread and are committed on a large scale, this type of illegal activities is one of the key elements of many illicit proceeds-generating schemes, and the income tax and value added tax are the most attractive targets for offenders. The international experts often highlight imperfection of the VAT system, since it is difficult to administrate, and possibility of offsetting the VAT on purchases provides opportunities for claiming VAT refund based on fictitious expenses.

In this context, consideration should be given to introduction of electronic invoices that would replace the currently used paper invoices. One of the advantages of electronic invoices is that they would enable to obtain up-to-date information on revenues and expenditures of companies and their counterparties. The use of electronic invoices should be the mandatory requirement for the widest possible range of business entities.

Besides that, special VAT deposit accounts are used in some countries, in particular in Azerbaijan. It is noteworthy that, under this mechanism, amounts of payable VAT are transferred through special accounts opened, for example, with the Treasury. Funds held on such accounts may not be withdrawn by a company at its direct request, but can only be used for paying VAT to its counterparties. Otherwise, these funds are withheld by the government as payments to the national budget. However, this method is not commonly used in practice so far.

2. Improvement of budgetary funds allocation system

Based on the provided information, it can be concluded that budgetary funds also constitute one of the main sources of funds used in illegal cash conversion schemes due to, *inter alia*, imperfect legislation governing the public procurement procedures.

Firstly, not all public (government) organizations procure goods, work and services in line with the general public procurement standards due to various reasons. Processes and procedures related to provision of services may be regulated by the internal documents of such organizations that do not provide for transparent and open competition among suppliers. Consideration should be given to application of the standard public procurement requirements to all public sector organizations.

Secondly, the LEAs practical experience shows that customers may misappropriate or embezzle budgetary funds by overstating the cost of purchased goods, work and services. Typically, additional factors and conditions are included in the technical documentation for artificially inflating public procurement contract cost, which makes it very difficult to determine whether or not the cost is actually overstated at the technical documentation approval stage.

Thirdly, in past, the public procurement legislation allowed for making procurements “from one source”, i.e. by signing contract directly with necessary supplier. At present, the legislation contains more stringent provisions governing this procedure, i.e. this method may be used in very limited circumstances. However, if it is possible to misuse this method in countries, it gives rise to high risk of illegal activity.

Fourthly, in some countries, primarily in the CIS member countries, the “delayed funding” practice is used, i.e. funds allocated from the national budget are transferred to regional and local authorities at the end of the first half of a year. As a result, in order disburse the allotted funds in a

timely manner, customers have to hold procurement tenders within the shortest possible time, which facilitates unfair competition.

3. Promotion of cashless payment practices

No less important, is promotion of cashless payment methods and reduction of share of cash in total money stock. This would help to decrease the share of shadow economy and would increase transparency of financial flows among financial and business entities operating in a country.

In this context, we think that countries should consider introduction of the mandatory requirement according to which only cashless payments shall be made under real estate property sale and purchase contracts.

4. AML/CFT and regulatory functions

It is proposed to consider the positive experience of the Russian Federation related to centralized exchange of information on high-risk customers among entities that are subject to financial monitoring.

In the situation featured by growing popularity of e-money systems, bookmakers' offices and online gambling sites, countries should consider possibility of decreasing the minimum threshold amount of transactions carried out through reporting entities. Countries should also give consideration to decreasing the minimum threshold amount of transactions that do not require identification of customers.

Besides that, it is expedient to create a national register of politically exposes persons for AML/CFT purposes.

4-1. Crypto currencies

At present, such means of payment as crypto currencies are commonly used in criminal schemes. Although FIUs may access unclassified (publicly available) transaction history log, their capabilities are insufficient for identifying crypto currency owners in practice.

In this context, it seems expedient to establish close operational coordination between FIUs and law enforcement agencies involved in detection and investigation into cybercrimes.

Besides that, information from open sources, including information posed on shadow financial service sites, indicate increased demand for conversion of legal entities' cashless funds into bitcoin-type crypto currencies.

5. Capabilities of FIUs and Financial Monitoring Units

First of all, it is obvious that, in order to enhance their capabilities, FIUs should have effective access to the widest possible range of government databases.

Effective access means not only request-response communication, but also integration of databases.

The FIU databases are interlinked with "external" databases of government authorities in many countries across the globe. Where direct interconnection is impossible, some FIUs use the so-called seamless integration technique.

This approach is based on the use of remote access point. However, unlike the traditional request-response communication pattern, the information system automatically requests data on each subject that is under examination. The received information is recorded into separate tables of the FIU database, which makes it possible to achieve databases coupling effect.

The wide range of available information enables to fully or partially automate the process of identification of suspicious indicators or characteristics without need for manual examination.

Entities that are subject to financial monitoring are, in turn, recommended to use the presented typologies and features as scenarios for identifying suspicious transactions. This will reduce the workload associated with analysis of high-risk customers' transactions.

Apart from laundering of criminal proceeds, operation of cash conversion schemes also causes serious damage to the economy of the surveyed countries, depriving them of additional resources for investment into social and economic development.

This study analyzes similarities and differences between the legislative frameworks of the surveyed countries. While most laws and regulations are elaborated and implemented in similar manner, there are certain differences that allow some countries to successfully mitigate risks

associated with misuse of cash for ML/TF purposes. However, it is impossible to assess the extent to which these risks are actually mitigated n practice in the framework of this study. All surveyed countries assess risks related to cash conversion for ML/TF purposes as medium and high.

The study also includes review of examples of financial investigations for categorization of the most common typologies of obtaining criminal proceeds and their laundering through cash conversion for further integration into legitimate circulation.

Based on the systematized typologies, we developed the characteristics of examined subjects and sources of qualifying indicators that require increased attention of reporting entities and FIUs in course of financial investigations.