APPROVED
By Order of the State Financial Monitoring of Ukraine
22 December, 2006, № 265

Typologies of legalization (laundering) of crime proceeds

in 2005 - 2006

State Financial Monitoring of Ukraine

TABLE OF CONTENTS

Executive Summary

These materials provide an overview of the trends and schemes of illegal income legalization, which were most widely used in 2005-2006. In particular, the typology includes the results of the research of state bodies – participants of the national system of counteraction to illegal income legalization (laundering) of Ukraine, as well as foreign experience. The typologies provide the examples of actual cases relating to illegal income legalization (laundering) (ML). These are most often mechanisms containing complex, complicated multi-chain transactions. One and the same scheme may contain transactions with cash withdrawals, purchase of securities, settlements with non-residents from off-shore zones/jurisdictions, fictitious foreign economic operations and illegal VAT repayment from budget; falsification of the documents, use of stolen passports, establishment of fictitious companies etc.

The examples of schemes are conventionally split into section, based upon the most "indicative" elements, to avoid duplication. The majority of examples are characteristic of every topic, because in the framework of this research the most typical set of ML tools, which are used, looks as follows: «fictitious firms – foreign economic operations (goods, services, securities etc.) – cash conversion.

The topics considered in sections 2-4 are the continuation of the typology research done in the previous periods (see "Typologies of illegal funds' legalization in Ukraine in 2004-2005).

The new sections 5-7 are separate.

In particular, section 5 concerns ML in the area of real estate.

Section 6 outlines the key risks for banking institutions regarding the involvement in ML processes (direct collusion with the employees of banking institutions, the use of court judgements, bank loans).

Section 7 contains the information regarding the types of ML via the use of such instruments as the Internet, payment cards, and non-commercial organizations.

The research was prepared on the basis of the materials of "Derzhfinmonitoring", National Bank, State Commission for Securities and Stock Market, State Tax Administration, Ministry of Internal Affairs, Security Service, General Prosecutor's Office, as well as open, in particular, foreign sources.

The said materials may be used by the subjects of primary financial monitoring to identify the ML risks, by law-enforcement bodies when holding investigations, as well as by other state agencies – participants of the system of counteraction.

1. General trends in legalization of illegal funds

During a long period of time ML has been positing one of major threats to economic security of the state. The greatest risk of ML is characteristic of the following economy areas:

- foreign economic activities;
- credit and finance;
- fuel and energy industry;
- metal and mineral resources market.

The "leader" among them is foreign economic activity (in particular, trade in high liquidity products, such as non-ferrous metals, chemistry, some types of agricultural products etc). As a rule, a part of exported shadow capital is later returned to the country as direct foreign investments. The following methods are used for the implementation of ML schemes:

- underpricing of exported products;
- overpricing of imported products;
- false import contracts, fictitious loan agreements etc.

During a long period of time export of capital via fictitious and "transit" firms[1], as well as various schemes associated with the export of cash, have been the principal ML schemes. At that, criminal groupings use more and more sophisticated ML schemes.

The most widely spread financial mechanisms used for illegal purposes through conversion and export of funds, are as follows:

- Crediting import operations, without entry of the product to the customs territory of Ukraine;
- Sale of the securities of the Ukrainian issuers by non-residents to the residents;
- Cross-border transfer of funds pursuant to enforcement documents, on the basis of court judgments;
- Payment of bills of exchange of the Ukrainian issuers, which are presented for payment by non-residents.

Note.

The majority of ML schemes are characterized by the participation of firms with attributes of fictitiousness (hereinafter – fictitious firms). The use of fictitious firms is widely spread in export and import transactions, in the activity of conversion centres, for illegal VAT recovery, securities, offshore transactions etc. More detailed information is provided in the annex.

---

[1] **Fictitious firm** is a legal entity having attributes of fictitiousness, which is established or acquired with a view to conceal illegal activity or carry out prohibited types of activity. As a rule, fictitious firms are established for a short period of time on the basis of forged documents, or registered on behalf of front persons, through the acquisition of an existing firm or establishing a new one (using illegal methods).

"Transit" firm is an actually operating legal entity, which underwent state registration, participating in the scheme as an intermediary and protector ("buffer").

At the same time, the risk of penetration and legalization of foreign criminal funds in Ukraine exists. If the participants of the national system for counteraction to ML ignore this threat, this can have a negative impact on the country's reputation.

As the experience of law-enforcement bodies shows, currently, the main volume of illegal capital is formed predominantly in the fuel and energy, agroindustrial complexes, and their legalization is effected through the credit and banking system, under the veil of foreign investments. In addition, public property and budget allocations for financial support and restructuring of companies, are often the subject of infringements by perpetrators. Apart from this, loss-making agreements are concluded, budget funds are used otherwise than according to intended purpose, as a consequence of what their embezzlement and large-scale fraud takes place.

Based upon the materials of the research of MIA

The following can be referred to as the key specific types of illegal activity in the agroindustrial sector of economy:

- Embezzlement and non-purpose use of budget funds, public and collective property;
- Infringement of applicable laws during entrepreneurship activity (absence and illegal obtaining of respective licenses and certificates for the right to effect commercial transactions with raw materials and finished products, illegal use of trade mark etc.);
- Illegal issue of certificates for the right to own shares of land;
- Evasion from the recovery of debt under loans obtained against the Government's guarantees.

Numerous violations of applicable laws are detected in the energy sector, taking place during the production, transportation and distribution of energy carriers, support of the function of energy-generating capacities, as well as in the process of denationalisation of the fuel and energy sector's companies.

At that, the officers of government and administration authorities get involved in the schemes of illegal activities more and more frequently, colluding with the representatives of commercial institutions with a view to obtain illegal income.

For example, managers of fuel and energy companies may deliberately enter into loss-making agreements with third-party organization, groundlessly grant loans to private organizations using public energy resources.

There is a trend of deepening criminalization of organizations supplying and selling oil products in the territory of Ukraine. In this connection, ensuring control over transactions under foreign economic contracts, including contracts with non-residents, remains a vital issue.

The most widely spread methods of illegal activity characteristic of metallurgy are:

- Groundless lending to commercial entities at the expense of public energy carriers;
- Monopolization of companies by separate financial and industrial groups during initial public offering and privatisation for the purpose of subsequent transfer of financial flows to offshore companies.

2. Cashing of Funds

The cashing of funds is, in itself, a legal transaction. However, the cashing of funds is used by perpetrators as an efficient ML scheme.

Currently, illegal conversion of cashless funds remains a rather profitable and widely spread type of illegal business for the servicing of organized crime. The key link in this process is firms having some attributes of fictitiousness, which are registered on behalf of front persons.[2]. One of the key objectives pursued by the founders of such business entities during their registration and use, is to evade criminal responsibility. For this purpose, front persons are registered as managers of fictitious companies.

Such firms are predominantly used by groups of persons having a significant experience of such activities and closely associated with credit and financial institutions. In such cases, the accounts of such companies are opened just at the banking institutions, which are under their control, and this enables full control over money flows going through the "transit" firm. Such mechanism guarantees secure implementation of further ML schemes.

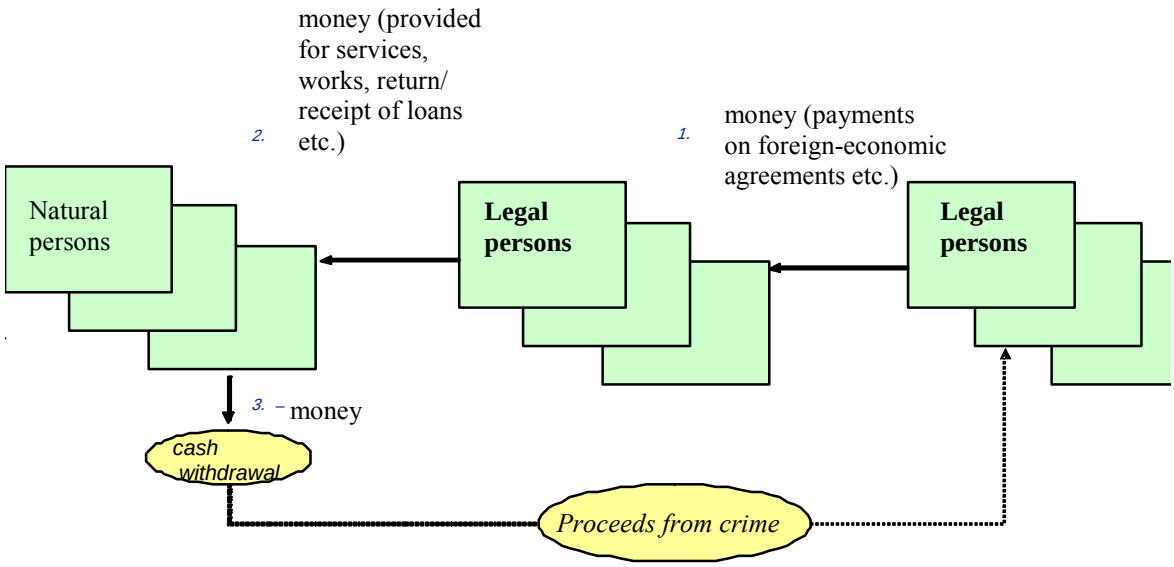
A sample scheme with cash receipt from the account (contribution), which can be associated with ML, looks as follows (see picture 1).

The final objective of the transactions is for individuals to obtain large cash amounts in the domestic or foreign currency from their accounts opened at local financial institutions. The said funds are received to accounts of private individuals in cashless form, as transfers from one or several legal entities, including from accounts opened with one and the same financial institution. The bases for such transfers can be different, including: payment under a contract, agreement, payment of remuneration for performed work, rendered services, transferred results of intellectual activities, transfer of bonuses, obtaining and recovery of loans, transactions with bills of exchange etc.

These funds, in their turn, can be received to the accounts of non-resident legal entities from both non-resident legal entities (mostly in foreign currency), and from resident legal entities (mostly in domestic currency). In the latter case, if foreign

[2] **Front persons** are the persons with whose help the financial transactions are effected directly or indirectly, for the purpose of ensuring the "breaking of chain" in ML schemes. Such persons can be used for the opening of bank accounts, transfer of funds both within the country and abroad, for withdrawal of large amounts of cash. When transactions are held, lost or forged passports/other documents, low-income persons' passports or documents of persons of no fixed abode are used.

trade contracts serve as the basis for settlements, as a rule, they contain incomplete or untruthful information. The settlements and the supply or transfer-acceptance of goods (work, services, results of intellectual activities) in the framework of fulfilment of obligations under the above-mentioned contracts, are effected on the same day, as a rule.



Picture 1.

Note.

When consecutive actions relating to transfer of funds are carried out within the same financial institution, another resident legal entity may be involved in this scheme, which performs the functions relating to accumulation of funds from other resident legal entities on its account, for their subsequent transfer to the account of a non-resident legal entity. In this case, funds from several resident legal entities that are the customers of both this lending institution, and other financial institutions, are received to the account of such resident legal entity daily. At the end of the banking day all funds credited to the account of this resident legal entity are transferred in full to the account of the non-resident legal entity (or the accounts of non-resident legal entities) for further transfer to the account (contribution) of the individual-non-resident/resident and receipt of cash funds.

The characteristic attributes of the transactions, ultimately aimed at obtaining cash from an individual's account (contribution), are as follows:

- With significant balances of cashless funds during the banking day, at the end of the banking day daily balances of accounts of the scheme's main participants are zero or small (not more than 5% of the daily turnover);

- Crediting of funds to accounts of individuals and cash withdrawals takes place on the same day;
- Coinciding details of the transaction's participants (for example, organizations' addresses);
- Regular obtaining of significant cash amounts by individuals-non-residents/residents from their accounts at the same internal unit of the lending institution (branch);
- Closing the accounts of persons involved in the scheme of receiving cash therefrom, upon completion of the full cycle of such transactions, or sudden termination of transactions with such accounts.

Some examples of criminal schemes, which have been identified by state agencies lately, are given below.

Example 1[3]*.*

Four citizens of Ukraine, against whom criminal proceedings were instituted for economic crimes, established a conversion centre. They registered a number of companies on behalf of front persons. The activities of those companies were fictitious in their nature, and financial and economic transactions were effected on paper only.

Within two years of such illegal activity, more than 200 companies of many of the country's regions have used the services of the conversion centre for the purpose of ML. The total volume of funds, "laundered" via the conversion centre, was over UAH 600 million.

Example 2[4]*.*

Three persons, a 30-year old Ukrainian, who was convicted for economic crimes before, and two of his close acquaintances, established a conversion centre for the purpose of rendering ML "services".

The fraudsters acted on the basis of the traditional scheme: funds under fictitious agreements were transferred via the accounts of transit and fictitious companies, which they opened on behalf of front persons. Low-income persons, on whose behalf the companies were registered, signed financial and accounting documents necessary for the operation of the criminal chain for a small amount of remuneration.

The officers of over 300 companies used the services of the conversion centre. The cash turnover of the centre was over UAH 200 million. At that, the "converters" received 3.5% of the amounts transferred pursuant to the criminal scheme.

Example 3[5]*.*

The criminal group, which operated a pawn shop, carried out illegal conversion of funds.

---

[3] Based upon the materials of the State Tax Administration of Ukraine
[4] Based upon the materials of mass media
[5] Based upon the materials of "Derzhfinmonitoring" of Ukraine and SSU

The «pawn shop» and Mr G. entered into an agency agreement, pursuant to which the latter undertook to find customers for the pawn shop, transfer the cash funds obtained at the pawn shop to the borrowers-individuals, and upon expiration of the loans' periods obtain the cash funds from them and return them to the pawn shop. Pursuant to this agreement, Mr G obtained the funds at the cash desk of the pawn shop and ostensibly transferred them under loan agreements registered by the managers of the pawn shop on behalf of front persons.

So, the cashless funds for UAH 160 million were transferred from the accounts of the pawn shop to the accounts of 10 individuals (based upon forged documents) as the "pawn shop's loan". Then a part of these funds for the amount of UAH 54.63 million was obtained in cash by Ms Ch. upon their order.

Later Mr G. and the pawn shop's employees prepared forged documents confirming the repayment of cash funds to the cash desk of the pawn shop, as repayment of a part of the amount of the registered loans. Another part was repaid (with the help of a securities' trader) through the transfer to the pawn shop of the bills of exchange for the product, which were issued by A Company, owned and headed by Mr G. The above-mentioned bills of exchange were issued for pseudo-commodity transactions, and did not have actual value, respectively.

Example 4[6]*.*

The persons who established 4 organized criminal groups dealt with illegal activities relating to conversion of funds. Each of them had several active members who acted as accountants and couriers of the conversion centre using the details of fictitious firms.

The group was managed by a 40-year old Ukrainian, having prior record of economic crime. Via a chain of fictitious firms, the cashless funds were cashed, with their further legalization through the construction of real property objects. In the two years of its activity, the number of the conversion centre's customers-existing companies of various regions of Ukraine – reached two thousand, while the annual volume of funds was almost UAH 1.5 billion.

Example 5[7]*.*

The conversion centre rendered ML "services" to the companies of one region of Ukraine. The centre was established by the director of a private company operating in a regional centre. Jointly with his friend, he registered a number of fictitious firms on behalf of front persons. Funds of doubtful origin were transferred via their accounts, and were later cashed. The total volume of transactions of the companies, which were part of the conversion centre, was over UAH 50 million.

Example 6[8]*.*

[6] Based upon the materials of the State Tax Administration of Ukraine
[7] Based upon the materials of the State Tax Administration of Ukraine
[8] Based upon the materials of the State Tax Administration of Ukraine

For the purpose of concealing illegal activities, a group of persons opened the companies having attributes of fictitiousness, which effected financial transactions aimed at concealing funds of illegal origin.

The companies «A» and «B» were not located at their legal and actual address and were registered on behalf of front persons. The officers had nothing to do with the financial and economic activities of the above-mentioned companies, did not sign any agreements or documents. They became owners of the companies for some financial remuneration.

The private company «A» obtained funds from the private company «B» as if the payments were made for information and consulting services, goods, materials, securities, mobile phone payment cards, repayment of the interest-free loan for the total amount of UAH 78.9 million.

These funds were transferred to the accounts of individuals (entrepreneurs who were stricken off the register), who subsequently withdrew these funds in cash. The said individuals granted loans for the amounts of over UAH 1–3 million to the company "A", which returned the funds to them under the veil of the repayment of interest-free loan in 3-6 days. So, the funds acquired a legal form.

In total, the company "A" transferred the amount of about UAH 67.2 million the accounts of individuals.

Example 7[9]*.*

Having a respective license, the private company "T" carried out operations with scrap iron. The company performed the following pseudo-transactions: the purchase of metal wastes from commercial institutions of two regions of Ukraine and then their reselling to a different commercial organization (the key supplier of this product to metallurgical companies of Ukraine).

In actual fact, after receiving payment for ostensibly supplied iron scrap, the perpetrators, under the guise of transit payment, transferred these funds via settlement accounts of the companies of the above-mentioned regions, to the address of firms having the attributes of fictitiousness. Therefrom they received the funds, which were already cashed, under the veil of payment for non-existent supplies, having paid 5-6% for the services to the "converters". Over the last years, the perpetrators have illegally converted at least UAH 4 million.

Example 8[10]*.*

The citizens of Ukraine established a fictitious company, which rendered the services to organizations of various spheres, specifically, ML services. In 2005, using bank accounts and details of "K" LLC, the above-mentioned persons carried out cashless financial and economic transactions between "K" LLC and other companies under their control. In this way, the funds obtained via fictitious firms for the total amount of UAH 903.0 were legalized.

Example 9[11]*.*

[9] Based upon the materials of the State Tax Administration of Ukraine
[10] Based upon the materials of the State Tax Administration of Ukraine

The managers of two private companies "A" and "H" carried out ML. Using a citizen's lost passport, they re-registered their companies on behalf of an unidentified person. In actual fact, this person was not involved in the scheme, only its passport data were used.

Later, with no intention to carry out financial and economic activity and for the purpose of concealing illegal operations, the managers of the said companies opened settlement accounts at a branch of a Ukrainian bank to carry out transactions on paper only.

At the end of 2005, the registration of the private company "H" was cancelled, as it had the attributes of a fictitious company. However, the offenders continued their criminal activities. Jointly with other business entities, they transferred significant amounts as payment for information and consulting services, commodities, materials, securities etc to the account opened by "M" private company at a bank. Then these funds were transferred to accounts of individuals, and the latter withdrew the funds in cash.

In this way, the officers of "M" company transferred to accounts of 9 individuals the funds for the total amount of UAH 335 million, out of which UAH 1.3 million was from the above-mentioned enterprises.

Foreign experience

Examples of the Russian Federation[12].

1. For the purpose of illegal cashing, the banking cash collectors' cars are often engaged in the scheme. Upon receiving the cash at the bank vaults, these cars directly deliver it to the customers, bypassing the banks. Using this scheme, two citizens of Ukraine "entered in the books" the amount of RUR 600 million within one day.

2. Based upon the information obtained from Rosfinmonitoring (Russian Financial Monitoring), [13]MIA of the Russian Federation, jointly with the law-enforcement agencies of Estonia, revealed the illegal activities of a commercial bank, which was headed by two natives of Syria and Palestine. In the ML scheme the fraudsters used foreign, including US, passports, as well as forged banking documents. In general, 230 transactions were carried out via accounts opened with the bank, for the amount total of RUR 14 billion.

3. During 2004-2005 via illegal currency conversion, the Russian bank laundered over RUR 48 billion, and RUR 1.5 was obtained on the basis of the lost identification document, which belonged to a teenager.

3. Foreign economic operations

[11] Based upon the materials of the State Tax Administration of Ukraine
[12] According to the data of the Association of Regional Banks of Russia and MIA of Russia
[13] Financial intelligence unit of the Russian Federation

Foreign economic operations remain one of the principal, most widely spread methods of ML. And a part of these funds is later returned to Ukraine, for their use in privatisation processes, in the secondary market of securities, purchase of land, real estate etc.

The export of capital outside Ukraine for the purpose of ML is carried out owing to the following:

- fictitious foreign economic operations[14], which are aimed at groundless repayment of VAT (a part of illegally exported funds is later returned from abroad for ostensibly exported Ukrainian products);
- contraband operations (the funds, which are illegally transferred, are used for the purchase of goods, which are subsequently exported to Ukraine at underestimated prices);
- Payment of dividends for the investments of non-resident companies, which are actually owned by the Ukrainian citizens.

Crediting of import operations, without entry of the product to the customs territory of Ukraine, is also often used in ML schemes; In this case, the resident enters into a foreign currency loan agreement with the bank, for foreign economic contracts for the supply of goods, pursuant to which the goods are not received to the territory of Ukraine (on EXW and CIP terms)[15]. The funds are transferred to the accounts of non-residents at foreign banks, based upon his order.

The standard scheme [16] with the use of pseudo export transactions looks as follows**Typical scheme**[17] of money laundering with the use of fictitious export operations is shown on Scheme 2.

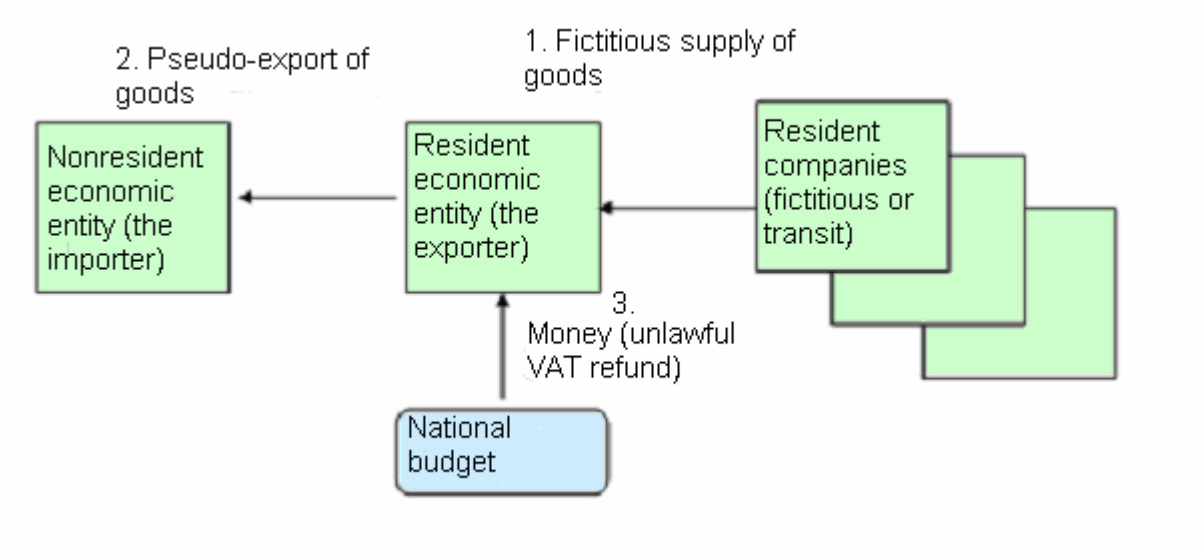
The real operating economic entity declares goods or other tangible assets (including unserviceable) supplied from the so-called transit or fictitious companies. Thereafter, the fictitious goods are, as it were, exported abroad, to the address of non-existing or created for the sake of this operation non-resident company, the export confirming documents being falsified. In addition, the export company may receive VAT refund from the budget.

[14] **Fictitious foreign economic operations** means fictitious export and import operations, which are carried out for illegal purposes and accompanied by falsification of the documents, which imitate the process of purchase and sale of goods, as well as the supply "by mistake" (agreements, cargo and customs declarations etc), and often accompanied by illegal VAT repayment from budget.

[15] **EXW** means an additional obligation of the seller to load the product into the buyer's vehicle; **CIF/CIP** is the buyer's need in additional insurance. The official rules for interpretation of trade terms of the International Chamber of Commerce (Incoterms-2000).

[16] За матеріалами МВС України

[17] According to information of the Ministry of Internal Affairs of Ukraine



Scheme 2

Often, the foreign economic schemes are of cyclic character (i.e. characterized by recurrence of cycles) and accompanied with embezzlement of budget funds through unlawful VAT refund (the so-called "carousel fraud").

Note.

During the last decade, the carousel fraud with unlawful VAT refund became a real threat for the EU member states. According to the estimates of the European Commission the annual amount of unlawful VAT refund in the EU member states reaches EUR 60-100 billion that jeopardizes the economic integrity and safety of the EU.

Hereinafter, the examples of illegal patters revealed by the competent government bodies in last years are given.

Case 10[18]

Company A paid for a huge batch of imported mandarins (28 thousand tons) on the basis of supply contract. In fact, the analysis of the documents showed that the fruits have been not been brought to Ukraine.

The goods were provided for being delivered from Hungary to Germany, to American company B. Company A paid for them to the account of Company B with Latvian bank.

In the foreign economic contract and CMR the quantity mismatch (about 1000 times) has been found that means the documents are falsified.

According to the information from the German competent authority the recipient of goods, as specified in CMR, was not officially registered. As a result, about USD 17 million were brought out illegally.

Case 11[19]

[18] According to information of the State Committee for Financial Monitoring of Ukraine
[19] According to the information of the State Committee for Financial Monitoring of Ukraine

Two Ukrainian import companies transferred abroad more than USD 28 million to a nonresident company as payment for goods. In fact, no goods were imported to Ukraine. For transferring funds denominated in foreign currency the importers presented to the bank falsified customs declarations.

Under the pretence of payments for foreign economic contracts the money came back to accounts of two Ukrainian export companies and then through buying bills and deposit certificates the exporters sent them again to the importers' accounts. The money was rolled over and over in several cycles.

This scheme allowed the swindlers not only to launder their money, but also to receive illegally VAT refunds from the national budget.

Case 12[20]

A criminal group legalized criminal proceeds using accounts of nonresident individuals opened with Ukrainian bank upon presentation of lost passports. Then money was brought out from Ukraine.

Money that was transferred to the above accounts with Ukrainian bank came from economic entities that seemed to be fictitious. The money was withdrawn from accounts on the basis of fictitious applications and brought abroad (basically, to Lithuania) on the basis of nonresidents' fictitious documents as an investment return.

The money withdrawn totaled more than UAH 750 million, about UAH 1 billion being brought out of Ukraine.

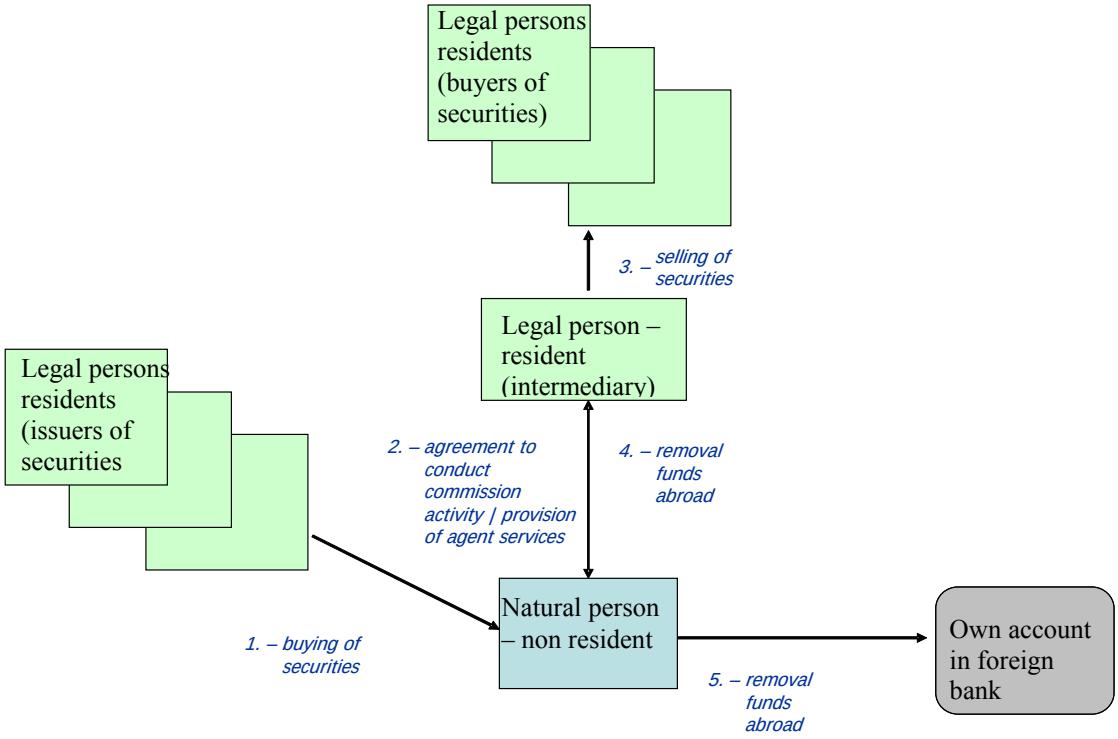
4. Securities (including interest in authorized funds)

Typical scheme of sale by nonresident individuals of securities purchased from Ukrainian issuers to other residents for the sake of money laundering is showed on Scheme 3.

Resident economic entity sells securities hold by nonresident individual on the basis of brokerage contract.

In fact, under the pretence of securities sale the entity accumulates dirty money from various Ukrainian companies that further is transferred to the account of nonresident holder and then to his/her account with foreign bank.

[20] According to the information of the State Tax Administration of Ukraine



Scheme 3

Note.

In case of the above scheme there is a high risk for banks of being involved in money laundering. If nonresident customer of the bank can bring a suit to a court for the bank's refusal of transferring a small amount (several thousand U.S. dollars) abroad without confirmation of previous investments, the court can award the bank to meet customer's demand in full (hundred dollars on the basis of the claim, ten million dollars thereinafter).

As of today, the most pressing problem are as follows: circulation of shares of non-existing companies and shares issued by companies whose issues were suspended or cancelled on the securities market, the use of illiquid shares of bankrupts for the sake of money laundering, non-listed shares and shares without real market value and their transfer to authorized funds of joint-stock companies.

As a rule, in the case of the above scheme, among entities dealing with securities trading there are nonresident individuals on whose accounts the funds are accumulated and further brought abroad under the pretence of an investment return.

Note.

According to the data of the State Securities and Stock Market Commission, in the first half of 2006, deals between securities traders and nonresident individuals, in particular, with nonresidents living in offshore areas, showed an upward trend. In the second quarter, nominal shares had a lion's share in the total amount of contracts (95.8% of the total contracts with nonresidents); the rest (4.2%) being represented by

other financial instruments, nominal investment certificates and nominal interest-bearing corporate bonds. Contracts worth UAH 4.8 billion were made at the securities exchange, the value of contracts executed on over-the –counter market totaling UAH 112.6 billion. Hence, securities are circulated chiefly on the over-the counter market.

For the purpose of legalizing criminal proceeds the criminals often use shares of open joint-stock companies circulated on the securities market. Recently, a large number of OJSC were founded through reorganization of limited liability companies, the authorized funds of the above OJSC being composed of shares of other OJSC entities worth several million hryvnias. New entities are established exclusively for the use of share issue for the sake of money laundering.

The typical scheme is described below.

The founders are dummies who agree to sign articles of incorporation upon request of unknown persons, for a certain remuneration, and have nothing to do with business. Actually, they do not either contribute any assets to the authorized fund or register the issue and place the shares.

Naturally, legal addresses of such companies are false inasmuch as they are registered on the basis of falsified documents. These companies neither perform any business activities, nor report to tax authorities and the SSSMC. They have no fixed assets or whatever real assets on their balances, their shares being used as a tool for illegal turn of funds in cash through the creation of fictitious authorized fund.

The use of bills and promissory notes may be very vulnerable to money laundering, insofar as their issue, as well as assignment, is not subject to registration by any authority. A money laundering risk of using bills on the securities market is connected not only with the fact that the bill can have an in-blank endorsement, but also with the bill's nature itself.

An in-blank endorsement is used, as a rule, for avoiding transfer of title to the bill when assigning it to third party through an agent (including, securities traders). In this case, the parties shall make contract, so the parties are identified. Bills of exchange and promissory notes can be issued only for documenting the debt for actually received goods, works or services. With the help of bills the criminals can create a fictitious debt and receive the legalized money, the more so as the issuer is a one-day company and the holder is a stakeholder of operation. It is very important to identify the way of bill transfer and persons involved, as well as to check whether goods, works or services have been actually delivered or provided.

Often, bills issued by Ukrainian companies may be presented for payment by nonresidents. In this case, there is a probability that banks transgress the applicable legislation of Ukraine and the NBU regulations for operations with bills of exchange and promissory notes.

Note.

Some banks fail to pay due attention to the study of financial status and solvency of the bill payer and person bearing liabilities on the bill with whom they make contracts and perform the operations. It increases a risk of being involved in money

laundering and is a breach of paragraph 3.1 of the Regulations for procedure of making operations with bills of exchange and promissory notes in national currency on the territory of Ukraine approved by the NBU's Board Resolution of 16.12.2002 №508 (hereinafter referred to as "the Regulations"). Contrary to paragraph 9.4 of the Regulations the banks substitute one type of assets (loans issued to borrowers) for other type (bills of exchange in the securities portfolio) and fail to keep registers of bills when performing operations therewith, as specified in the Regulations and appendixes 2, 3, 4, 5 and 6 thereto[21].

The typical scheme with the use of bills is as follows.

The bank's customers, resident who ensures the cash outflow, and nonresident, made a contract that provides for full or partial payment by bills, then, on the resident's account the funds are accumulated from various Ukrainian economic entities, the initiators of cash outflow, under fictitious contracts or through purchasing bills at an unfair price. Thereafter, nonresident presents bills for payment to the resident who orders the bank to purchase foreign currency on the interbank market and to transfer the funds abroad.

In addition, when legalizing proceeds with the use of bills the bills may be paid under fictitious contracts with further withdrawal of cash from dummy loan accounts in the likeness of consumer loans.

For this case **the typical scheme** is as follows:

Funds to be turned in cash are transferred to the account of a front commercial entity. On its behalf a bill for the whole amount is written and avalized by servicing bank under the contract on securities payment. On the basis of a certificate the bill is delivered to other front company as if payment for works done. This scheme allows the criminals to transfer funds from settlement account of the company to the internal bank account ("Other payables on operations with bank's customers"). Thereafter, the bank pays cash to a dummy as a consumer loan in amount specified in the bill. The borrower is other fictitious company, a holder of the bill. Later, it repays the loan to the bank by a bill received from the former fictitious commercial company. In fact, the bank writes off funds from its internal account in amount specified in the bill as repayment of consumer loan.

Below, some cases of criminal schemes revealed by the competent government authorities in recent years are given.

Case 13 [22]

Employees of close joint-stock company B misappropriated the company's funds and changed the owner in the following way: the company's top officials decided to increase its authorized fund through additional issue of shares worth UAH 2.15

[21] The NBU's letter of 16.03.2006, N 43-212/1546-2736

[22] According to data of the State Tax Administration of Ukraine

million. These shares were purchased by some enterprises and insurance companies who received the control under the company. A portion of funds received from sale of shares (UAH 650 thousand) the top officials took over and further legalized through transferring them to the account of a front company under non-existing assignment contract.

Case 14 [23]

For the purpose of provisioning several Ukrainian insurance companies purchased shares of heavy-industry companies A, B, C, and D. In fact, the above companies were incorporated exclusively for the use of shares issued as a tool for money laundering and seemed to be fictitious.

Nonresident corporations were involved in the purchase and sale of shares.

Further, the criminals using requisites of fictitious companies A, B, C, and D, registered issue of shares worth UAH 279.6 million presenting to the SSSMC the falsified documents. Later, these funds were legalized through transferring to the individuals' accounts with Ukrainian bank.

Case15[24]

A group of nonresidents (basically, passport holders of the Russian Federation, Moldova, and the Baltic States) transferred FX funds abroad with the use of the following criminal scheme. These individuals were registered in Ukraine as self-employed persons and opened accounts with one Ukrainian bank. After that, through the securities trader, they sold bills of companies from various regions of Ukraine that were either fictitious or liquidated by court decision. The total value of contracts reached more than UAH 1.5 billion.

The similar schemes allow the large importers to legalize dirty proceeds, in particular, through understating the real value of imported goods.

Case 16[25]

During a long while the limited liability company A performed securities trading through fictitious nonresidents. Totally, more than UAH 500 million was transferred to their accounts with Ukrainian banks under the pretence of purchase of shares. Later, these funds were transferred to accounts with Baltic banks as an investment return.

Case 17[26]

Ukraine's resident, Mr. F, received illegal money from acting as an employment agent (placed Ukrainian citizens in job in European countries). In the Czech Republic, he earned EUR 85 thousand and then legalized them by purchasing at the special auction 10% shares of OJSC B at an understated price of UAH 207 thousand (while the par value thereof was more than UAH 820 thousand). He paid in cash. The

[23] According to data of the State Tax Administration of Ukraine
[24] According to information of mass media, including UNIAN
[25] According to the data of the State Securities and Stock Market Commission of Ukraine
[26] According to the data of the State Committee for Financial Monitoring of Ukraine

declaration attached to the application for purchase of shares contained false and misleading information. In addition, it was found that the director and the founder of OJSC B was Mr. F's relative.

Case 18[27]

Top officials of company A are misappropriating funds and legalizing them as expenses on payment of the fictitious bill issued under the fictitious contract.

Company A for the purpose of funds converting makes a fictitious services contract with fictitious company B and pays to the latter by the domiciled bill that specifies the place of payment which is different from the payer's location. In agreement with employees the company A opens a bill account.

The conversion of funds is hidden in two ways:

1. Company A sends the funds to the bill account with endorsement "for domiciliation of bill". The domicile bank transfers these funds to the account of company B thereby paying the domiciled bill.

2. The domiciliation contract contains not settlement account of company B, but an account opened for the name of dummy X («Individual demand deposit») in order to complicate countercheck of relations between companies A and B.

Company B accepts the bill issued by company A and collected by the bank, the bill having an endorsement that the funds from this bill shall be transferred to individual X contracted by company B for providing consulting services to company A. This is done for avoiding a direct correspondence between the settlement account of company A and the account of individual X, inasmuch as such operation may draw attention of law enforcement bodies.

Having transferred funds from the account of company A or from the account of company B to the account of individual X., the dummy receives cash at the bank and gives the major portion thereof to Company A, the rest (from 5% to 12%) being paid as commission fee to the participants of the conversion contract.

According to the NBU data[28], some members of securities market pursue an investment policy connected with investing funds into non-listed and illiquid shares.

Notes. Some banks register operations with securities disregarding their economic nature or failing to identify their real value to avoid provisioning. As a rule, the banks overestimate the securities. As a result, the banks imitate an increase in positive financial result.

The NBU analysis of banks' statistical reports has showed that, in 2005, investment in securities grew 1.8 times (while the total assets increased 1.6 times). More than 60 per cent of banks increased their operations with securities. Moreover, nearly every seven bank increased its securities operations 4 - 7 times, whereas some of them 17 – 40 times.

At the same time, methods specified in interbank bank regulations for determination of fair value of securities (non-listed on the regulated market) not

[27] According to the data of the Ministry of Internal Affairs of Ukraine

[28] The NBU's letter of March 16, 2006, N. 43-212/1546-2736

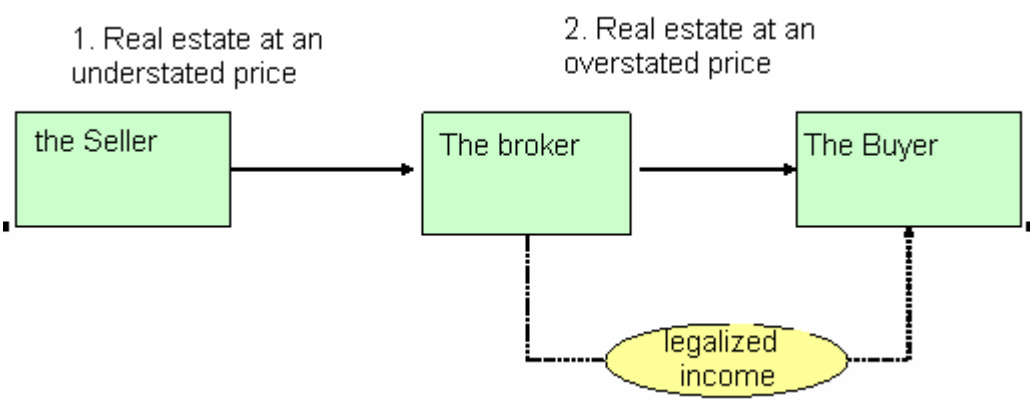
always meet requirements of the international accounting standards and cannot ensure the true fair value of securities.

5. Real estate

Gerrymander and fraud in real estate trade is gaining more and more significant scale. Criminals launder their dirty money due to the operations on purchase-sale of real estate, make investments in the housing construction and receive the real estate in ownership illegally.

For instance, **the typical scheme** of money laundering with the use of speculative operations in the real estate trade looks like this (see, circuit scheme 4).

An agent purchases an object at a low price for the money obtained in the criminal way and repurchases it to the criminal at a much higher price. Difference between the purchase and sale price makes a legalized income. In other words, money is legalized due to the real estate overpricing. A cyclic object repurchase, as well as participation of "transit", fictitious companies, may be a distinctive feature of the scheme. In this case, the real estate evaluation documentation and purchase-sale contracts may be falsified.



Scheme 4.

Some examples of criminal schemes revealed recently by the competent government bodies are given further.

Case 19[29]

Mister K., an American, who resides in Ukraine, received on his account with the Ukrainian bank a significant amount of money (several hundred thousands of U.S. dollars). The mentioned funds came from abroad from other foreigner, Mr.T.

According to the information of competent authorities, Mr. T. was directly engaged in the illegal drug traffic and money laundering at the international level. Mr. K. departed from America to avoid punishment for committing a crime.

Mr. K. spent the money for purchasing apartments. By the way, Mr. T. was a former owner of some of them.

[29] According to data of the State Committee for Financial Monitoring of Ukraine

The apartments were repurchased at price much more different from the purchase price (overpriced or underestimated). In particular, there were untrue data as to object contract when repurchasing one of Mr. K's apartments.

Case 20[30]

The top officials of company D installed equipment in the hospital. According to the acceptance documents, the works were made duly and in full. Respectively, from the hospital's current account the budget funds worth UAH 417.8 thousand were transferred to the enterprise's account. However, actually, the works on the equipment installment were not made and the money transferred were converted in cash and misappropriated.

Moreover, the mentioned company D concluded a construction contract with other enterprise according to which it received UAH 40.1 thousand. In fact, the object to be constructed was already put in commission in the previous year (nearly seven months ago).

Due to its unlawful activity the company D illegally received funds worth UAH 457.9 thousand and used them in the enterprise's financial and economical activities.

Case 21[31].

Mr. M., the Chairman of the Supervisory Board of open joint-stock company A for the purpose of misappropriation of the company's assets, made up a fictitious protocol of the Supervisory Board Meeting on transferring the railway line to CJSC B (worth UAH 674 thousand). This asset was owned by OJSC A, but at that time it was used as a tax mortgage.

Contract on dismounting of the line was signed by Mr. M. personally on behalf of company X, as though it were an enterprise that financed the works on dismounting and transportation of line to CJSC B, but in the accounting records of the OJSC A amortization of the property was not fixed.

The stolen line was sold by Mr. M. to other company Y for UAH 82 thousand with the help of private businessman according to the concluded contract on selling the CJSC B's products. Having received the funds on his account, the private businessman withdrew the money from the account in cash and handed them over to Mr. M. For these "services" the businessman received commission fee for which later he purchased a car.

This scheme was realized by Mr. M. with the assistance of the officer of a district taxation inspection.

Case 22 [32]

Company A received a certificate for a property share of the reformed Ukrainian enterprise B. The company A officials sold it to the private enterprise C. However, the funds were not divided between the shareholders and were used in the financial

[30] According to the data of the State Tax Administration of Ukraine
[31] According to the data of the State Security Service of Ukraine
[32] According to the data of the State Tax Administration of Ukraine

operations for "personal needs". During inspection the fact of money laundering worth UAH 195.6 thousand by the director of company A was established.

Example 23[33].

Ukrainian company A obtained credit in foreign currency for acquisition of land for construction of cottages. A foreign citizen acted as pecuniary guarantor therewith. Company B also obtained investments from non-resident company C for acquisition of construction land. Companies A and B converted the money obtained into Ukrainian currency and transferred it to individuals for acquired pieces of land. Most of them lived in dormitories and were under 25 years old.

In turn, the individuals were acquiring these pieces of land from members of gardener associations as agricultural land. The money the individuals obtained was used for enlargement of their accounts, transfers to deposit accounts, payment for services, credit granting, making contributions to statutory fund, bond acquisition.

Thus, a change of designated purpose of land use didn't take place in the process of its selling, i.e. the agricultural designation remained. This gives evidence of violation of existing legislation and occurrence of money laundering.

Foreign experience [34].

The CEO of a bank created a criminal group of four bank officers using his official position. He withdrew systematically the money he was entrusted with amounting to about three milliards Russian rubles according to financial experts' estimates. Some part of withdrawn money was invested in acquisition of real estate in Vladivostok. Inter alia, 27.69 million Russian rubles were laundered as first installment for acquisition of the entire building.

7. Bank institutions

Substantial possibilities of financial and credit sector, concerning use of modern technologies for wealth management, make it attractive for direction of efforts of organized crime.

Unlawful obtaining (granting), withdrawal, as well as unauthorized use of credit and budget means still remain the main kinds of law violations in the credit and banking sector. Fabrication of data related to business and financial performance of companies, pledged property (assessment of its value or existence), and mechanism of fictitious bankruptcy are used actively therewith. Frequently such crime is carried out with the direct or indirect participation of the officers of financial and bank institutions.

[33] According to records of the State Financial Monitoring Service of Ukraine

[34] According to information of the Ministry of Internal Affairs of Russia

As the current trends show, taking into account ongoing activities of criminal groups on money laundering, banks are the best instruments for transactions of such kind. The most widely used technique of money laundering is uncontrolled monetarization of non-cash resources. In such a case cash transactions have quite legal appearance.

Moreover, international experience verifies that wire transfers are one of the means, which can be used for laundering of money both within and beyond the state boundaries.

The analysis of wire transfers plays the main role in the majority of financial crime investigations starting with detection of the source of funds and ending up with ascertainment of links between launderers, terrorists/ terrorist organizations and other associations, organizations or countries.

In order to provide security of banks against such criminal practice, it is necessary to implement a set of measures, the main of them being:

- careful examination of clients, especially the ones of the risk groups as well as ascertainment of links between the participants of transaction, including other clients;
- smoothly-running monitoring of money transfers, including the procedure of its receipt;
- watchful treatment of correspondent banks (do not establish relations with the ones that don't have physical existence in any country).

Moreover, revelation of and counteraction to unlawful schemes are possible upon monitoring of financial transactions under the external economic contracts of the bank's clients, open-faced securities that are not placed on depository, and under the condition of cooperation with duly authorized agencies of other states, as well as in cooperation with customs, tax and other law enforcement agencies of Ukraine.

Conspiracy with a bank institution

One of the typical schemes of money laundering with participation of bank institutions looks as follows (see Fig. 5).

An organized criminal group includes bank officers and two companies – paper company B (conversion) and company A.

Bank officials prepare in advance application of client B to close his operating account. This serves as a reason for crediting of all funds received within one transaction day to corresponding bank account X (allegedly by the agreement on supply of goods, provision of works or services by company A to B).

As a result, conditional "lack" of money on the current account of paper company B is being provided during the working day of a bank institution in the case there is threat of the bank inspection or freezing of accounts of paper company B.

Upon bank's close-down the application is being destroyed and the money is being transferred to the current account of company B, whereof they are directed to conversion in cash. In this case accounting records on the movement of funds on the account X are being destroyed as well.

Conversion transactions are carried out upon close-down of the monitoring units of the bank and before the close-down of the Clearing House of the National Bank of Ukraine. Agreement between companies A and B, payment documents and expenditure papers serve a basis for carrying out of such shady transactions.

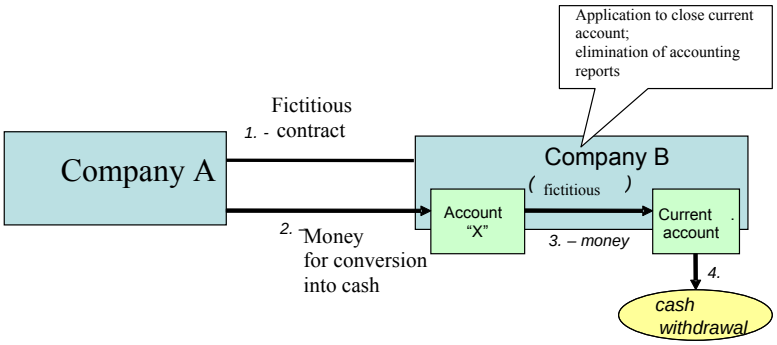


Fig. 5

Below there are some examples of criminal schemes revealed by state agencies within last years.

Example 24[35]*.*

Criminally conspired with the branch CEO of one of Ukrainian banks, the leader of a criminal group set a full system for obtaining credits through the offices of agents. The system involved over ten affiliated companies. Defrauders arranged for credits secured on property being assessed by real estate agency affiliated to them as well. As a result thereof, overall value of pledged property turned out to be overstated almost 20 times compared to its actual value.

Offenders were transferring the criminal money to the accounts of paper companies and later used them for acquisition of real estate, cars and shares. Within the few years the criminal group laundered about 29 million hryvnias.

This scheme involves a high risk of abstraction of bank funds (credit).

Example 25[36]*.*

A public utility company employee being in the meantime the founder of a number of private enterprises and the employees of one of commercial banks exercised money laundering through allegedly performed works and procurement of agricultural products. The money was drawn from the account of the company by means of cheques. In general the offenders laundered over 300 million hryvnias.

[35] According to the records of the State Tax Administration of Ukraine
[36] According to the records of the General Prosecutor's Office of Ukraine

Foreign experience

Examples from the Russian Federation [37]**.**

1. The Ministry of Internal Affairs of Russia initiated a criminal case against Project Crediting Bank (PCB) suspected of money laundering offense. According to information obtained in the course of investigation during the year of 2005 the bank laundered about seven billion Russian rubles. For this purpose the senior management of PCB used the schemes with the participation of a network of fly-by-night companies. The companies, through which the unlawful financial transactions were carried out, were registered on lost or stolen passports.

Note.

In May 2005 the Central Bank revoked the license of PCB for violation of the AML law. Particularly, PCB didn't send to the Federal Financial Monitoring Service of Russia the reports on transactions subject to mandatory monitoring. Reports on particular transactions were sent with delays. Moreover, the bank violated the customer identification procedure.

2. A criminal group practiced money laundering. The group was led by a godfather, the citizen of Georgia. He had false passport and stayed in Russia illegally. Moreover, his passport was issued on the basis of imitated stamp of registration.

The group carried out unlawful bank transactions associated with money laundering, conversion into cash and outflow of currency resources abroad – to Georgia, Latvia and the US. The offenders also obtained the budget means to the amount of over three billion Russian rubles within the agricultural programme related to hog production.

The money flaws were laundered by means of four commercial banks, their licenses were revoked hereinafter. The money "processed" by commercial banks was obtained predominantly from unlawful financial transactions, banditry, functioning of casino and withdrawal of budget funds. The daily income from unlawful bank transactions alone exceeded five hundred thousand US dollars.

Five shell "non-commercial" organizations took part in the process of money laundering in addition to banks.

3. A citizen of the People's Republic of China (PRC) on behalf of one of the largest banks of PRC involved funds of individuals and legal entities without bank accounts being opened, and carried out payment transactions. However, he was not authorized by the bank to carry out bank activities and bank transactions in Russia, he didn't have the registration obligatory in such case and license to carry out bank activities and bank transactions in Russia. Within three months the offender earned income of almost 143 million rubles.

Court Decisions

[37] According to information of the Ministry of Internal Affairs of Russia

Offenders also use unlawful schemes of writing funds off the correspondent accounts of Ukrainian banks abroad for debts of their clients. These schemes can be used successfully for the purpose of money laundering. In fact, the courts of foreign jurisdiction levy unrightfully the funds from a bank towards repayment of its client's credit debt to the third person.

According to the information of the National Bank of Ukraine some Ukrainian banks have been already affected because of implementation of such schemes. At present there are cases of initiation of proceedings in the CIS countries (in Moldova, Belarus and Russia).

During the last years the mechanism of use of court decisions obliging banks to purchase foreign currency on their clients' instruction without observation of requirements of the Rules of Currency Exchange Transactions on the Inter-bank Currency Market of Ukraine (Regulation of the Board of the National Bank of Ukraine of March 18, 1999 # 127) expanded as well.

Note.

In particular, the documents verifying the previous transfer of funds to Ukraine in the form of foreign investments; money orders on payment of duty for mandatory pension insurance or bill of entry are not provided. This affords a possibility not only to lead without difficulty extremely large amounts of capital beyond the bounds of Ukraine but to avoid compulsory charging, deduction and payment of the duty for mandatory pension insurance they are required.

Lawsuits, in which a defendant may be a Ukrainian legal entity or a non-resident assigned a claim to this subject, are being initiated beyond jurisdiction of Ukraine.

A typical scheme of use of court decisions concerning bank institutions in the schemes of money laundering consists in the following.

A resident - a client of a bank - and non-resident enter into any external economic contract, the conditions of which are neglected by the resident. As a result the non-resident goes to the law and the court decision holds the resident to pay the non-resident a certain amount of money. On the basis of the decision a bank purchases currency on the inter-bank currency market of Ukraine and transfers it abroad.

Foreign courts verify artificially created debt of the Ukrainian company to the non-resident (including the one located in the offshore zones) and resolve to deduct in behalf of the latter the funds located on the correspondent account of the bank serving his debtor client. In addition, the legal proceedings take place without notification of that bank and mature with operative rendering of decision, opening of law enforcement with ulterior garnishment and seizure of funds from the correspondent account.

Note[38].

In order to prevent possible negative consequences connected with forced writing the money off the correspondent accounts of Ukrainian banks for debts of their clients and considering possibility of biased approach to handling by foreign courts of disputes relative to protection of rights of Ukrainian entities,the National Bank of Ukraine offers:

- to study in detail the legislation of the countries of the foreign banks during establishment of correspondent relations with them, the interstate agreements settled to regulate these relations, as well as to treat watchfully the business reputation of a correspondent bank;

- to provide for arbitrary language in the contracts on establishment of correspondent relations with foreign partners, according to which the disputes between correspondent banks will be handled in the procedure of international commercial arbitration by competent judicial authority chosen by the parties.

- to draft a provision in the contract on establishment of correspondent relations, according to which the banks are not liable for obligations of their clients, when Ukrainian banks open accounts in the foreign banks.

Bank loan

Bank institutions may become an object of criminal acts during provision of services of credit granting. Hereinafter such funds may be laundered using typical schemes.

There are lots of scenarios of abusive acts using bank credits, including in particular:

- fabricated letters of guaranty, as well as provision of collateral on behalf of non-existing (fictitious) company;
- pledged property that is artificially understated or just fabricated that is not owned by the collateral or has been already bonded;
- fabrication of the financial standing/income level of the person being granted a credit etc.

Banks are being badly damaged by pettigoffing loans, inasmuch as in the most cases it is not possible to recover money obtained by offenders. In this case express credits, when the borrower within a couple of minutes obtains money for goods or formalizes a credit card directly in the shop, are the riskiest product. In this case a bank is unable to carry out good verification of creditworthiness; the decision is made by the electronic screening system on the basis of personal data. Offenders, in turn, examine the nuances of credit formalization, particularly of corresponding questionnaires. Offenders use dummy individuals to simplify the implementation of the schemes.

The typical methods of credit fraud include as follows:

1. Dummy individuals.

[38] According to the records of the National Bank of Ukraine (the letter of February 3, 2006 # 18-312/424-1252)

An individual (typically impecunious) formalizes to his name credit in a bank or in a shop for a modest remuneration. The offenders assure him therewith that it is not necessary to redeem the credit considering their connections with the right people. The borrower gives money or goods purchased on credit to offenders; they pay him promised remuneration and disappear. It is almost impossible to achieve debt repayment and find true offenders in such cases.

2. Forged documents.

The offenders paste their photographs in fabricated (stolen/lost) passports or change their appearance to correspond the one in such document. As a rule, female passports are used in such cases, since women can easily change their appearance.

3. Conspiracy with the representatives of credit institution who influence the decision on credit granting.

For offenders conspiracy with the credit manager is the most effective way of fraud. Bank officer will always stand by and correct the data in the questionnaire. Moreover, in this case the original passport is not necessary (copy of the document is enough).

Below there are some examples of criminal schemes revealed by state agencies within last years.

Example 26[39]*.*

Company D acting in Ukraine as a dealer of the foreign company N entered on behalf of the latter into a contract on supply of equipment with company K. Company K obtained a credit in a Ukrainian bank for execution of the agreement. Obtained amount of credit was transferred to the account of company N to a foreign bank as upfront payment. In the meantime company N obtained a credit in that bank securing its repayment with funds specified in the contract with the Ukrainian company K.

Consequently, the funds obtained did not proceed to the account of company N and were received by the bank straightly as repayment of the credit. After a while (one-two weeks) company N declares bankrupt and reorders itself into other structure. The liquidation commission doesn't present company K in the list of creditors of company N, inasmuch as the money of company K are not detected on the account of company N.

Example 27[40]*.*

On the security of bank A, company F obtained in bank B a credit, the funds of which were distributed between the senior management of company F and bank A and appropriated. Upon maturity of payment and correspondently non-repayment of credit funds by company F, bank B complains to companies guarantor – bank A. The latter formalizes and grants company F with a credit to the amount of money necessary for repayment of the debt. In this case red ink transaction of the bank alters to active transaction.

[39] According to the records of the Ministry of the Internal Affairs of Ukraine
[40] According to the records of the Ministry of the Internal Affairs of Ukraine

During the time gained the credit funds may be used in the criminal scheme. For instance, as a result of transactions carried out with appropriated funds an income was earned, which enabled repayment of the debt.

Example 28[41]*.*

Company A opened a deposit account in a bank and having transferred to that account five thousand hryvnias it obtained credit to the amount of four thousand hryvnias on the security of the account. At a later stage company A returned funds from the deposit account to another person on the basis of the fact that funds were credited to the account by mistake. Later it turned out that company B was registered on the nominee names.

Company B presented this very bank a personal cheque to the amount of thee thousand hryvnias. Using these funds company B carried out a number of transactions and obtained credit to the amount of 1500 hryvnias on the security of its balance. At a later stage it turned out that company B was registered on the nominee names. The cheque the company B presented was forged as well.

Example 29[42]*.*

Mr. N, the owner of the agricultural private enterprise A settled an agreement with a bank on opening of credit line to the amount of 200 thousand hryvnias and obtained credit in full. His own holding valued at over 500 thousand hryvnias served as security for this agreement.

At a later stage Mr. N registered company B with a purpose to avoid repayment to creditors. This company was assigned with pledged property (according to purchase and sale agreement) without knowledge and participation of the creditor bank. The documents were filled with consciously inveracious data concerning debtor's debt on the part of company B connected with transfer of this property.

Correspondently, enterprise A, having laundered these funds, didn't repay the debt to the creditor due to non-availability of assets and was declared as bankrupt.

7. Other trends

Internet

The number of cyber crimes is increasing more intensively as compared to other types of crimes. The felons are not aiming, as it used to be, at attracting attention, but are concentrated on obtaining money in the roguish way. They are cracking databases more and more often and pretend identities. Moreover, internet-technologies are more and more frequently used in the schemes of ML.

The most popular fraud trends in the Internet are the following:

1. Shady transactions at the network auctions. (Purchasing items at the false auction sites. The items, purchased at them, are never delivered to the clients).

[41] According to the records of the Ministry of the Internal Affairs of Ukraine
[42] According to the records of the Security Service of Ukraine

2. Delivery of cheaper goods, than were ordered, or poorer quality goods, purchased in the on-line shops.

3. Nigerian Advance Fee Fraud (AFF) (or "Nigerian letters" one of the classical network frauds).

The e-mails are distributed, in the body of which the recipient is asked to assist in transferring dozens of millions, hidden in the safe place, to a definite banking account (in freely convertible currency), for which the promised remuneration makes 10-20% of the total sum. At that the felons ask to supply the accounts requisites and sometimes even the copies of identifying documents. The clients, who accepted such "business proposals" before execution, lose dozens and hundreds of thousands dollars.

4. Money withdrawal from credit cards for non-executed Internet-services.

5. "Pyramidal" proposals as for outwork, which promises incredible income.

6. Credit shady transactions. (The credits are offered with preliminary payment of interest: the interest is transferred, but the credit is not transferred on the account.)

7. Proposals on opening a cheap credit card, a condition of which is the advance fee or personal data disclosure. (In reality the card is not open, the advance fee "vanishes", or the frauds just lift the money from the clients' accounts).

Note.

Particular anxiety of the law enforcing bodies is caused by the fact that more and more frauds in the Internet are executed by the organized criminal organizations which operate on an international scale. At that, the majority of cyber-criminals is Russians by origin or come from other countries of the former eastern bloc. In particular, the frauds demand money from the owners of the web-sites, threatening to destroy the site, if the owner does not pay the money. The owners of the British casinos have become victims of such racketeering of late. An attack of this kind brings the frauds income 10 to 30 thousand dollars.

The frauds, connected with the elaboration of computer viruses are quite popular at the moment alongside with stealing company information on the competitors' request. In accordance with the data of the agency Reuters cyber-crimes already in 2004 left behind drug trafficking by its "profitability".

For instance, in accordance with the research data of the antivirus company McAfee, the most widely-spread cyber-crimes in Russia are cracking computer networks, racketeering, and also criminal schemes of ML in the network and usage of phishing technologies. The list of the major trends of the cyber-criminal activities is more various in the USA: apart from the above-mentioned, such crimes as credit shady transactions, frauds with the credit cards, blackmail are often registered.

In accordance with the data of Security Exchange Commission of the USA (SEC) there are an increasing number of internet-brokers clients' complaints on the occasion of breaking up their online accounts, which is done by hackers from Eastern Europe. Many crimes of similar nature were organized via the borders of the USA, especially from Eastern Europe, Russia, Ukraine. SEC collaborates with the law-

enforcing bodies of these countries, but application of off-shore schemes by the frauds complicates the detection of criminals.

The internet users themselves and also employment of their accounts and actions, which are carried out as a result of the delusion, present good means for arranging such schemes as ML alongside with other crimes.

At the same time it is very difficult to investigate the crimes in which the Internet is so actively involved both due to the electronic character of the transactions and due to the international character of relations, when in the corresponding schemes participate, as a rule, anonymously, citizens and criminal groups from different countries. It is not without purpose that different countries consider the issues in the sphere of ML control both on the level of law-enforcing bodies and in the framework of special international agreements.

Note.

In 2006 Ukraine ratified the Supplementary minutes to the Convention on cyber-crimes, which pertains the criminalization of the actions of racist and xenophobic character, performed via computer systems (Law of Ukraine №23-V dated July, 21, 2006).

At the moment one can observe the increase in the volumes of e-mails distribution and number of sites aiming at offering easy money. These may be attempts to employ users in the capacity of "drops" (another name is mules) - users, whose accounts are used for laundering money, obtained by means of cyber-crimes.

At that the **typical scheme** is the following:

The users are offered a well-paid job, connected with the Internet, which doesn't require any experience or qualification. At that the registration for work requires some personal data and the number of the banking account, at which money transfer remittance is received. Then the "drop" is asked to put money (of criminal character) for some fee to his/her banking account and to transfer it to another.

With the aim of avoiding involvement into such schemes, the internet-users are recommended to:

- ignore messages and sites, which offer extremely easy and well-paid job;
- not to grant any personal data (passport number or social security number, etc.), which may be used for opening banking accounts in their names;
- in the case you have doubts before contacting a company, which offers a job, get reliable information about it.

Among the most malicious kinds of network shady transactions, the financial fraud under the name "phishing" occupied the leading position[43].

As a rule, the criminal **scheme** is realized in such a way:

[43] Phishing is creation of the exact copy of the existing Web site (e.g., banking site) with the aim of making the user insert his personal, financial data or the password. Mass mailing and/or decoying the users to the fake Web site are used in the process of phishing.

The organizers of phishing distribute letters in the name of technical specialists of well-known banks, internet providers and Payment System, in which they make reference to system failure and offer the users to "remind" their password, requisites of their credit cards and social insurance cards and so on. For that, in most of the cases they create a copy of financial sites, with the help of which they collect the financial information. Then the criminals withdraw the money from their victims' accounts and try to legalize it, transferring money via different electronic payment systems, in the result of which it is practically next to impossible to identify the origin of the costs.

Note.

In accordance with the data of APWG[44], the most attractive goal for the felons is the financial sector (in 2005-2006 over 85% of all effectuated attacks fell to it). The tendencies of the last years testify to the steady geographical preferences of the felons: as to the choice of registration of phishing sites these are the USA, China, Korea, Brazil, Germany, Great Britain, etc.; to the leading countries in which the felons use special software and viruses for phishing, apart from the USA, China, Korea and Brazil, refer Spain, Russia and Romania. The increase of phishing sites outstrips the increase of the number of electronic messages from phishers. In the first quarter of 2006 the number of phishing-sites increased almost by 2,3 times as compared to mid-quarterly indices of the previous year (28,5 thousand and 12,4 thousand accordingly), and the messages from phishers almost by 1,24 times (53,5 thousand and 43,2 thousand accordingly). Judging by the APWG-experts opinion, such a substantial increase is stipulated by the emergence of so-called "phishing-whales" - universal software utility which allows creating a phishing-resource in the short period of time.

So, with the aim of possible losses prevention and risk minimization against phishing the staff and clients - card owners of the bank in the case of receiving corresponding messages on their personal mail boxes have to ignore these messages and don't have to open any references inside these messages and also not to forward any personal data (debit or credit card number, PIN-code, social insurance number) in answer to the request of the electronic message from any organization or a private individual: he/she also has to check monthly report, submitted by the bank with the aim of confirming all the transactions.

One more **typical scheme**, used by the hackers, is obtaining the owner's name and password with the help of a special "spy" software, effectuating access to his account and remittance of the received costs via mediators to the banking accounts, which are used for ML, for instance, by means of buying the shares of a small company with the aim of further speculation-sale as soon as they manage to raise price on them at the market.

[44] The working group on phishing control (Anti-Phishing Working Group, APWG) studies the problems of this phenomenon and finds the ways of counteraction and registers the facts of such kinds of fraud.

Some examples of funds lifting, detected by the state bodies of late, which may be used for succeeding ML, are listed below.

Example 30[45]**.**

Some unknown individuals placed "doubtful" announcements as for granting services on selling credit cards with stolen PIN-codes on one of Ukrainian information portals (under the same alias and with identical feedback references).

For more detailed explanations of buying and selling conditions to the potential clients there was created a site with the Russian domain. The conditions of operation handling and the subject of buying and selling testified to the high risk of stealing client's money.

The conditions of payment fulfillment envisaged the transfer of funds via the systems Western Union and WebMoney under the "sellers" requisites. The form of the order delivery was courier or checkroom. Besides, the clients were requested identification data (passport and also a photo), and likewise a pre-pay (in the case of credit cards - 100%).

Example 31[46]**.**

In 2006 the trial in San Francisco (USA) sentenced the person of Ukrainian extraction, Mr. V., to nearly three years of imprisonment. Mr.V. pleaded guilty for spreading thousands of unlicensed programs via Internet. Only in the course of one transaction via the Lithuanian bank the hacker legalized 20 thousand US dollars.

Example 32[47]**.**

A criminal group operated in Russia and Ukraine, which stole funds from personal banking accounts of the French.

Frauds stole over 1 million Euros with the help of "sleeping viruses". As a result of such operations only one client of the bank lost 40 thousand Euros.

On infecting the victims' computers with viruses, the felons got control over their banking accounts and lifted it within a couple of seconds.

The virus was introduced via the e-mails or internet-sites and remained inactive until the user checked his banking account. As soon as he did it, the virus came into an active stage and registered the password and banking codes, which were later sent to the malefactors. The criminals checked if the victim had any money on the account, after which they transferred the money to the third person ("drops") who for a small commission making 5-10% agreed to transfer money via their accounts. But sometimes such transactions were carried out without the privity of "drops", as a result of which the factual detection of the source of the funds origin becomes impossible.

Taking into consideration high risks of using banking services, which are provided via Internet, with the aim of ML or terrorism financing, the NBU

[45] Materials submitted by the State Information Monitoring of Ukraine
[46] Mass Media materials, including. Interfax and magazine "Korespondent"
[47] Mass Media materials, including «The Guardian»

recommends the banks at granting such services to use adequate measures for the realization of Basel principles, concerning the risk minimalization as to the banking product. Special attention should be paid to the financial transactions in the case of[48]*:*

- change of the transactions character, which are carried out with the help of Internet-banking usage;

- considerable change of counteragents on such transactions;

- realization of similar transactions, which haven't evident economic sense, with the same counteragents.

Charge Cards

The international experience testifies to the fact that nowadays payment technologies (charge cards, Internet system, mobile payments, etc.) are very popular and convenient in use but at the same time they are very vulnerable and liable to usage with the aim of ML and terrorism financing. At that, the major danger is the international providers of new payment techniques, but not the ones, that operate within the boundaries of one country.

Note.

With the increase of plastic charge cards, losses from fraud in the world with the help of such instruments are becoming more and more palpable. The frauds with the help of plastic cards of the system Visa and Europay steal nearly 2 billion dollars annually worldwide. Such crimes are most frequent in the countries, where financial instruments of this type are quite spread, but the special state security forces haven't learned yet how to effectively control any shady transactions connected with them.

Machinations with plastic cards may become a successful "starting line" for the realization of ML scheme.

The experts enumerate over 30 ways of stealing money from plastic cards. More than half of crimes in this sphere are eventuated by the so-called scheme "absolute counterfeit of the card". For example, in the store or at a restaurant the owner is given a fake card as soon as the authentic one has got into the hands of a waiter or a salesman. This mode is most frequently practised in the countries of South-Eastern Asia and also some European countries: Spain, Italy and Great Britain.

The rest most spread kinds of fraud are the following:

1. Obtaining the cards requisites with the aim of its further usage for the purchases in the online-shops. At that one shouldn't necessarily make a fake copy of the card.

One of the schemes of obtaining information from the card is the usage of psychological methods by the malefactors. The schemers get the information about the clients, who own large sums of money via their informers in the banks and then later, pretending to be a bank employee, come to such clients' places (home or work) and ask to transfer money via another bank, in which they also have an accomplice. A

[48] Letter of the NBU dated January, 10, 2006 N 48-012/29-192

request of this kind is explained, as a rule, by some unexpected technical failure at the bank. At that the malefactors give the account number, to which the money should be transferred, and they bring papers, made by the informer of the bank, to confirm it. As a result they receive both the transferred money and the number of the client's card, which gives the possibility to further purchase goods at client's expense.

2. Unauthorized access to the account.

It must be noted that unauthorized break of the banking information systems is quite complicated technically and is connected with definite risks. Larceny via Internet is a perspective trend but until now is not sufficiently profitable in Ukraine, as opposed to other European countries, in the first place due to the insignificant volumes of such financial operations.

3. Larceny or usage of the lost plastic cards.

At that the stolen or lost charge card is used by the individual for settlement transactions, for instance, for a single or serial purchase of light industry goods, which are later resold. The purchase is made directly or incognito (by ordering it via Internet).

As a rule in the case of the charge cards theft the probability of the quick disclosure of the crime is quite high, as one can trace a distinct tendency in the immediate change of the character of purchases, which are made practically perpetually until all the funds on the card are exhausted. In the case when only the information about a card is stolen, then the character of purchasing activity is quite disguised and may have several cycles.

Note.

The status of the confidential banking information, spreading of which may cause harm both to the bank and the clients, is determined on the legislative level in Ukraine. The protection of the electronic information in the process of banking operations procedure is regulated by the laws of Ukraine and by the regulatory documents of the NBU, in which there is a defined complex of protective measures applied to electronic banking information on all the stages of its creating, processing, transferring and storing. Confidentiality is achieved by means of obligatory implementation and usage of the special means of safety ensuring (technological, bookkeeping means, cryptographic and organizing means).

Some examples of criminal schemes, exposed by the state bodies of late years, are listed below.

Example 33[49]*.*

Company "K" received refunded VAT for the amount of 2, 9 million hrivnias (for the court decision execution). The next day the whole sum was transferred to the enterprise "L" as a payment for the scratch-cards. However, as it turned out legal proceedings on bankruptcy were instituted against the individuals "K" and "L".

At that company "K" bore some fictitiousness features. The legal address of company "K"'s registration was the real address of the habitable flat, the resident of which had no connection to the company.

[49] Materials submitted by the State Information Monitoring of Ukraine

Foreign experience.

Examples from the Russian Federation[50].

1. In Moscow ceased its existence the criminal group, which was dealing for six years with the production and realization of the fake registration permits, customs seals and banking plastic cards. According to the preliminary information, via the branched network of offices, which belonged to the malefactors, up to 7 thousand clients were served by them. The daily income of the malefactors made up not less than 240 thousand dollars and the annual up to 70 million dollars.

2. 22-year-old citizen of the republic Belarus with the help of computer technologies usage sold fake means of payment having injured banks in different countries worldwide at the sum of 15,1 million US dollars. He had nearly 70 serious clients from Russia, Moldova, Ukraine and also from the countries of Europe and the USA. Among 37 banks which suffered losses in such a way, are the banks from the USA, France, Switzerland and Luxemburg. The malefactor removed the information from the banking plastic cards and sold it to the clients. He found hackers, capable of obtaining this information, indicated where it could be found and later processed and resold the information to the buyers.

Non-profit organizations

To the peculiarities of non-profit organizations (NPO), which are attractive for usage in criminal schemes, we refer, in particular, the ability to accumulate funds via membership dues, donations and so-called non-profit activity and to spend the money in cash on the realization of projects and on acquisition of necessary equipment.

It is very difficult to trace the machinations in this sphere and to prevent them due to the nature of such organizations (especially statute functions) and due to the loyal system of state regulation and control in different countries. Having obtained the status of charitable ones and having freed from taxes, they can be used for ML of the territorial money transfer via affiliates or for the physical infrastructure support of terrorists (directly or as a cover for their actions).

The following measures are necessary for preventing the use of NPO for illegal purposes:

- control over large transactions (especially if charitable foundations are involved);
- distinct demands to the registration of charitable and other NPOs, in particular foreign and/or at establishment of non-residents, and state control over their activity.

Some examples of criminal schemes, revealed by the state bodies in late years, are listed below.

Example 34[51].

[50] Based on the data of Ministry of Internal Affairs of Russia and "Interfax"

The Ukrainian charitable foundation conducted very many financial operations with the participation of different economic entities. The money was transferred to the accounts of other companies and then further was withdrawn in cash. On the completion of operations the Foundation disappeared, which gives grounds to suppose its factious nature. The scheme included near 60 participants (the ones who directly conducted doubtful operations and also circumstantial participants of the given chain).

Example35[52].

45-year-old Ukrainian arranged the activity of conversion centre, which operated in the banking and finance sphere. The schemer registered two all-Ukrainian invalid associations with the aim of ML and its further transfer into cash. These companies didn't effectuate any statute functions; they only served for conducting non-commodity operations. Using requisites of these associations and of several other fictitious firms, also created by him, the malefactor conducted a chain of non-commodity operations at the sum nearly 2 million hrivnias.

Example 36[53].

The officials of the charitable foundation created a criminal organization, which operating on the principles of "financial pyramid" dealt with attracting the voluntary dues of the citizens. By means of transactions to the account of a fictitious company 329, 3 thousand hrivnias was legalized and used further for individual purposes.

NPO and terrorism

Easiness, with which many charitable non-governmental NPO may cross the borders and act in any (including those that are at enmity) countries, make them quite vulnerable for unlawful use by the terrorist groups. In many countries the legislation on the issues of charitable activities is poorly worked out and in some others the legislation is defined by separate states, which complicates the coordination of actions, in its turn allowing the corrupt NPO to operate without being punished.

The risk of using the territory of the country for providing the terrorist activities (for the concealment of terrorists, creation of business structures, which finance the terrorist groups, acquisition of the mass destruction weapons, etc.) is inherent not only to the regions, seized by the military conflicts in which terrorism and drug-dealing greatly influence the creation of political situation, but for any country to some extent.

The international experience testifies that the risk of using NPO, for charitable foundations in particular, with the aim of terrorism financing is quite high.

---

[51] Materials submitted by the State Information Monitoring of Ukraine

[52] Based on the materials of STA of Ukraine

[53] Based on the materials of STA of Ukraine

Thus, the experts of FATF note that in many cases just charitable foundations themselves were involved in the terrorism complicity.

To the financial operations, which indicate the connection with terrorism and which especially concern NPO, we refer:

- participation in the operation conduction of persons, involved in terrorism, weapon trafficking, illegal migration (including refugees, persons with illegal registration) both direct participants and founders and partners - legal entities.

- the direction of cash-flows and/or pertaining of the participants of the operation to the "crisis" zones of the world: territories (countries) in which separatist and fundamentalist movements are in operation, also countries in which no measures are taken to stop terrorism/ML financing alongside with those in which the state control is loosened;

- use of informal money remittance;

- illegal use of the intellectual property (fraud assisted by the use of e-mail, in particular, is based on the "Nigerian" scheme and also the sale of piratical software, including CD-and DVD-disks);

- cash transactions (so-called mode of "swallowing" at which the funds should not be transferred via the banking structures).

The "doubtful nature" of NPO can be reflected by some other operations, apart from above-mentioned (including foreign economic ones), by the volumes and direction which is not typical for the statute activity (e.g., operations with securities, namely acquisition of a big block of shares from the non-resident and its further reselling, allotment of consulting services to the enterprise; operations in the sphere of travel business).

Abbreviation list:

ML – structuring (laundering) money, obtained in an illegal way
SEC- Security Exchange Commission of the USA
STA – State Tax Administration
NPO – non-profit organization
SS – Security Service

Supplement

Using companies with features of fictitiousness in ML schemes

Use of fictitious companies is characteristic for actually all big schemes of LM, including legal entities with features of fictitiousness. Often companies are established for short-time period on the grounds of fictitious documents or on behalf of fictitious persons. These companies are transferred criminal assets, which later are exchanged and transferred to the accounts of 'pocket' companies located in tax heaven countries. These organizations legalize criminal proceeds through accounts of different companies.

Particularly, in Ukraine one could officially register a company aiming to legalize criminal proceedings. At the same time during inspections of such companies the fictitious features of them may be identified. As a rule, fictitious companies are established through purchase of existing company or establishment of a new one (through illegal procedure).

Period of operations of such companies could vary from some days to some years. In some cases their avoid tax registration; while they could carry out business operations and possess a seal and bank account. Some companies may even provide tax reports for some time. Here everything depends on the aim of the fictitious company existence.

Characteristics of companies of features of fictitiousness are as follows:

- absent information about real operations of the company as a business entity (in a country of registration);
- impossibility to reveal real physial location of the company employees and CEOs (trustees, reporesentatives) as well as its activities;
- obvious inconsistency between the company bank transactions and tax payments;
- integration of functions by a founder, CEO and chief accountant in one person.