ЕВРАЗИЙСКАЯ ГРУППА
по противодействию легализации преступных доходов
и финансированию терроризма

EURASIAN GROUP
on combating money laundering
and financing of terrorism

WGTYP (2012) 8

1 - November - 2012
English – Or. Russian

For Official Use

17th EAG PLENARY MEETING

November 5 – 9, 2012

India, New-Delhi

MONEY LAUNDERING AND TERRORIST FINANCING VULNERABILITIES OF TRANSACTIONS WITH INTANGIBLE ASSETS (PARTICULARLY, INTELLECTUAL PROPERTY)

For any inquiries, please, contact the EAG Secretariat:

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

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

Table of Contents

Introduction

Following the meeting of the Working Group on Typologies (WGTYP) held on November 23, 2011 during the 15th Plenary Meeting of the Eurasian Group on Combating Money Laundering and Financing of Terrorism (EAG) Ukraine was designated to steer the typology exercise: Money Laundering and Terrorism Financing Vulnerabilities of Transactions with Intangible Assets (in particular with Intellectual Property).

The need for researching the issues pertaining to transactions with intangible assets is dictated by lack of such studies in the past and also by the enhanced risk of the use of these tools for the ML/FT purposes.

The main goals of this typology exercise are:

- Studying the legal framework that governs the registration and circulation of intangible assets in various countries;
- Identifying the most vulnerable elements of transactions with intangible assets and compiling the list of the basic criteria of risk of their misuse in illegal transactions;
- Comparing approaches to identification and analysis of shady transactions with intangible assets that could be related to ML and FT;
- Summarizing the practices of investigations of ML and FT cases involving transactions with intangible assets.

Taking part in the research were the Financial Intelligence Units of the Russian Federation, the Republic of Kazakhstan, the Republic of Uzbekistan, the Republic of Belarus, the Republic of India, the People's Republic of China, the Republic of Tajikistan, the Kyrgyz Republic, the Republic of Turkmenistan and Ukraine.

1. General

Definition

For the purpose of this typology research intangible assets are defined as non-monetary assets that have no physical existence and are properly documented, evaluated and are capable of producing economic benefits to an entity over a long (more than 12 months) time.

Intangible assets include the assets that meet the following conditions:

- Lack of physical or material existence;
- Possible links to other assets/property;
- Used for manufacturing products, performing work, rendering services or for administrative needs of an entity;
- Used over a long period of time, i.e. over 12 months-long useful life or during standard operating cycle if it exceeds 12 months;
- Capable of providing economic benefits (income) to an entity in future;
- Availability of properly issued documents certifying the existence of the assets and the exclusive right of an entity to the results of intellectual activities (i.e. patents, certificates other titles of protection, patent, trademark, etc. assignment (acquisition) agreement).

Use of Intangible Assets

Today, intangible assets are widely used in various sectors of economy. Intangible assets were initially designed for addressing the problem of difference between the book value and the market value of companies. However, as they were more widely used, intangible assets evolved into the separate tool that allowed market players to optimize their financial flows.

In this context, intangible assets have dual nature. First of all, they are used for accounting valuation of the market value of company's competitive advantages (patents, brand names, know-how, etc.) used for managing company capitalization and making administrative decisions. This aspect of intangible assets is of no interest in the context of this research since it is the component of large, often transnational, manufacturing, telecommunication or retail companies that are well known and recognized in the market.

The other aspect of intangible assets, which is of greater interest in the context of this research, is their potential use as a separate tool in market transactions involving redistribution of the derived benefits among the market players. Given the possibility of subjective estimation of their value, intangible assets have become the lucrative object of commercial transactions, i.e. the tool for redistribution of financial capital.

Types of Intangible Assets

Intangible assets may include the intellectual property objects such as:

- Literary, artistic and scientific works;
- Performance rights of actors;
- Audio records;
- Radio and TV shows;
- Inventions in all areas of human activity;
- Utility models;
- Commercial prototypes;

- Trademarks, service marks, brand names and trade names;
- Other rights to the results of intellectual activity in the manufacturing, research, literature and art areas;

and also:

- Business reputation of an entity;
- Licenses;
- Quotas and other similar assets.

Vulnerabilities

Since intangible assets have no physical existence and their price formation is opaque (nontransparent) the fairness (legitimacy) of the transactions with such assets may be in doubt.

In course of investigations of transactions with intangible assets one should keep in mind that all business transactions of an entity shall be properly reflected in the tax and accounting records.

Thus, transactions with intangible assets are featured by the following vulnerabilities which should be subject to special attention:

- Intangible assets (design, copyright certificate, patent, etc.) shall be properly documented and their owners shall have the right to dispose of them, i.e. such assets shall be subject to sale and purchase;
- Intangible assets shall be legally certified and have actual price (value);
- Intangible assets shall produce income and shall be supported by the documentary proof (certificate) of their acquisition (creation, holding).

Possible overvaluation and fictitious deals, especially related to transfer pricing, make intangible assets the attractive tool for money laundering and terrorist financing.

Potential Risks

Given the aforementioned vulnerabilities, there are the following risks of misuse of intangible assets for carrying out illegal transactions:

1. Financial risks

Due to imperfect pricing mechanism intangible assets may be a useful tool for perpetrators in pursuing various illegal goals; including the use of intangible assets in the ML schemes:

- For giving semblance of legitimacy to income (royalty) of individuals (e.g. to those associated with public officials);
- For removing funds to foreign jurisdictions;
- For reducing tax burden for a business entity.

2. Legal risks primarily related to:

- Recognition of intangible asset as such;
- Recognition of title (ownership right) to intangible assets.

The Civil Codes, Tax Codes and other special laws of the countries define intangible assets as the outcomes of intellectual activity and the rights to their use, the rights to use

property/ natural resources, brand names and trademarks. The necessarily condition is the use of intangible assets for the manufacturing purposes, or for rendering services (capability of producing economic benefits (income) to a taxpayer), or for the administrative purposes.

The comparative analysis of the surveyed countries' legal and regulatory framework pertaining to registration of title to intangible assets and their further circulation shows that the countries apply the similar (identical) approaches to the regulation in this area.

In particular, the following countries have the separate government regulators:

- The Russian Federation (the Federal Service for Intellectual Property);

- Ukraine (the State Intellectual Property Service of Ukraine);

- The Kyrgyz Republic (the State Intellectual Property an Innovation Services under the Government of the Kyrgyz Republic);

- The Republic of Uzbekistan (the Intellectual Property Agency of the Republic of Uzbekistan);

- The Republic of Belarus (the National Intellectual Property Center of the Republic of Belarus).

The issues pertaining to ownership of intangible assets and their circulation by non-resident legal entities and individuals are regulated in a standard manner established for all parties to such transactions (in the Russian Federation, Ukraine, the Kyrgyz Republic, the Republic of Uzbekistan and the Republic of Belarus).

In general, despite the comprehensive regulation of the issues pertaining to registration of the title to intangible assets and their further circulation in the surveyed countries, the main vulnerability is the risk of subjective valuation of such assets by the market players and difficulties in monitoring fairness (legitimacy) of transactions with such assets.

2. Offences and Typologies of Money Laundering Involving the Use of Intangible Assets

Typically, the schemes of money laundering with the use of such tool as intangible assets are very intricate and complex. In such situations, intangible assets serve as the useful tool for funds redistribution.

In this context, the main weakness of intangible assets is their subjective pricing and the problem of their actual existence. In some cases perpetrators intentionally use more complex ML schemes involving intangible assets by engaging additional intermediaries or by using financial instruments that disguise the true nature of their transactions. Such transactions shall be subject to special monitoring by financial intermediaries.

It should be noted that such transactions may be related to both the primary offence and money laundering.

The most common offences committed with the use of intangible assets include:

- Forgery of documents certifying the right of ownership of intangible assets;
- Illegal copying of information with further sale of such information on a regular basis;
- Production and sale of products under trademark without obtaining permission of the relevant patent holder;
- Use of technologies that are intellectual property of other company;
- Theft of data and their further sale.

2.1. Offences Involving the Use of Intangible Assets

Presented below are the examples of typical offences committed with use of intangible assets:

2.1.1. Illegal Distribution of Software and Video

The most wide spread offences involving infringement of the copyright legislation are those related to software sales. Such offences are usually committed by copying CDs or by selling software through the controlled websites.

It should be noted that such offences in aggregate account for a significant portion of damage inflicted on the software developers.

2.1.2. Sales of Online Content

The scheme is, to a large extent, similar to that used for sales of content through the cellular communication operators. The difference is that perpetrators directly breach the copyright legislation and offer to download intellectual property objects. Payment for such services is arranged through the special SMS messages of the cellular communication operators. The obtained funds are laundered by making payments under fictitious intangible assets use contracts to the controlled companies.

It is noteworthy that in case of application of the fraudulent schemes involving intangible assets and services of mobile communication operators, such operators are held liable neither for the actions of perpetrators, nor for the composition of the sold content.

2.1.3. Sales of Stolen Databases

After obtaining, in an illegal manner, the copies of the databases of the government authorities or (typically) large companies, offenders distribute such copies among customers or competitors for deriving profits.

2.1.4. Trademarks

As the services involving sales of information and entertainment content by the cellular communication operators become more popular, perpetrators also become more active in this market segment.

After establishing the partnership relationships with the cellular communication operators, (mala fide) companies offer various information and entertainment services intentionally misleading buyers about the cost of such services (cost of downloaded content).

2.1.5. Tax Offences with the Use of Intangible Assets

In Ukraine, the Russian Federation and the Kyrgyz Republic, the issues pertaining to taxation of transactions with intangible assets are regulated by the Tax Codes. Since valuation of intangible assets is subjective, the issues concerning the use of transactions with tangible assets for minimizing tax liabilities still raise questions in these countries.

For example, the RF legislation contains implicit provisions that allow legal entities that are the RF tax residents to use financial transactions with intangible assets for minimizing their tax liabilities. However, such phenomenon is not typical in this jurisdiction.

The most wide spread scheme of minimizing tax liabilities through transactions with intangible assets involves getting tax credit and reducing the amount of profit tax through accrual of depreciation when companies purchase intangible assets (software, licensed products) from the "shadow" economy companies at excessive price, while the products are actually delivered at lower price.

In course of audits it is virtually impossible to identify the manufacturer of such software since it can be an individual who does not declare his/her activities or a legal entity that supplies more computer products than it declares.

As for minimization of tax liabilities through transactions with non-residents, special attention should be paid to issues related to payment for the rights to use copyrights, patents, registered trademarks, know-how, etc..

2.2. Money Laundering through Intangible Assets

At the same time, all aforementioned offences may also be related to money laundering, and transactions with intangible assets may be used for giving semblance of legitimacy to the flows of criminal funds.

It should be noted that financial transactions that are related to money laundering and involve the use of intangible assets closely resemble typical methods of money laundering through trade operations, i.e. overstated/understated cost of goods and services, manipulation of quantity and quality of goods and services, etc.

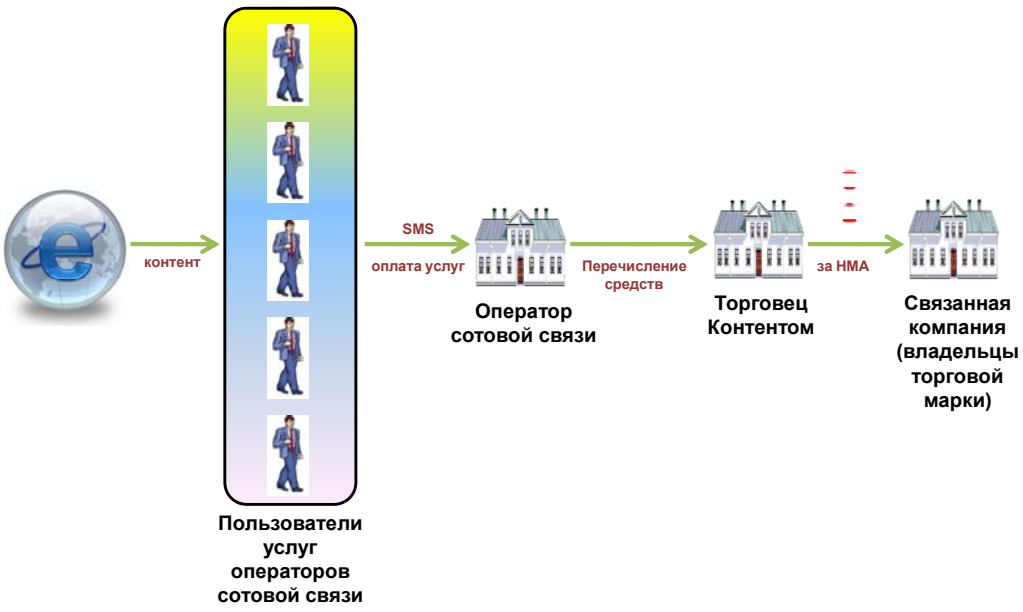
In 2006, the FATF conducted the typology research – Trade-Based Money Laundering.

The most common method of transferring illegal funds between entities is overpricing of intangible assets.

In order to be able to identify such schemes the financial intermediaries and the financial intelligence units should more thoroughly analyze the information.

2.2.1. Laundering of Criminal Proceeds from Transactions with Online Content

Figure 2.2.1



Контент	*Content*
Пользователи услуг операторов сотовой связи	*Mobile communication operators' subscribers*
SMS оплата услуг	*SMS payment for services*
Оператор сотовой связи	*Mobile communication operator*
Перечисление средств	*Transfer of funds*
Торговец контентом	*Content vendor*
За НМА	*For intangible assets*
Связанная компания (владельцы торговой марки)	*Associated company (trademark owners)*

This diagram shows the process of obtaining funds through payment by individuals for content via the use of mobile communication operators' services.

Later on, these funds are accumulated and transferred as payment for various intangible assets. The complexity of the scheme is that it is necessary to estimate cost of such intangible assets. The risk posed by such schemes increases if money launderers further engage companies incorporated in other jurisdictions.

Typically, transfer of funds to companies registered in other jurisdictions has advantages since the involved intangible assets do not physically cross the border and, therefore, there is no need to file additional documents with the customs authorities.

It should be noted that other intangible assets like databases, software and other types of intangible assets may also be use as content.

Thus, the money laundering scheme may involve various components.

2.2.2. Laundering of Criminal Proceeds from Illegal Debiting Funds to Subscribers' Accounts

Perpetrators illegally debit funds to the accounts of mobile communication operators' subscribers.

In order to launder the obtained proceeds perpetrators register, in advance, the rights of ownership of intangible assets (e.g. brand name) in the names of the associate companies and under the pretext of use of such intangible assets transfer proceeds to such companies.

Thus, the income received by the associated companies looks apparently legitimate.

Figure 2.2.2.

Пользователи услуг операторов сотовой связи	*Mobile communication operators' subscribers*
Оплата услуг	*Payment for services*
Оператор сотовой связи	*Mobile communication operator*
Перечисление средств	*Transfer of funds*
Торговец контентом	*Content vendor*
За НМА	*For intangible assets*
Связанная компания (владельцы торговой марки)	*Associated company (trademark owners)*

It should be noted that such schemes are designed for stealing funds from a large number of mobile communication operator customers.

The amount of illegally debited funds is often small enough for a victim to apply to the law enforcement agencies. And even if a victim applies to the law enforcement authorities that amount of stolen funds is insufficient for instituting criminal proceedings, which certainly plays into the hands of perpetrators.

2.2.3. A money laundering scheme involving the sale of a fictitious online casino

The popularity of online banking has resulted in a sharp rise in hacker attacks on bank customers who manage their bank accounts online.

After taking possession of online account management passwords, hackers transfer the money from these accounts to the accounts of individuals they control for subsequent cash withdrawal through bank institutions pay offices. As evidence of legality of such operations, a customer (natural person) presents to the bank a contract for purchase of an online casino along with a description of the website and gaming tables.

After obtaining some additional information, the FIU established that such online casino does not exist and that funds were taken from accounts as a result of hacker attacks.

Fig. 2.2.3[1].

As an additional source of information when dealing with such schemes, it's necessary to pay attention to such things as online communication with the customer, namely the location of his IP address.

[1] Компания А - ***Company A***
Украденные деньги - *Stolen money*
Подставное лицо - *Straw man*
В банке представлен контракт на покупку-продажу интернет-казино - *A contract for purchase of online casino is presented to the bank*
Остановленная операция - *Terminated transaction*
Наличные денежные средства - *Cash*
Банк - *Bank*

2.2.4. A money laundering scheme involving patents

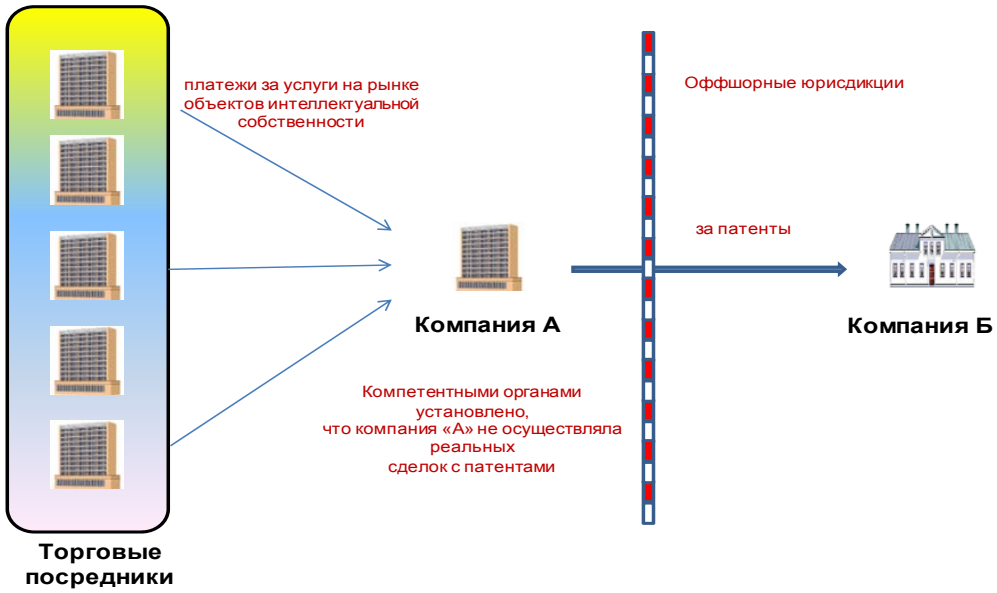
A group of individuals set up Company A that allegedly provided services in the intellectual property market.

Later, this Company A transferred large amounts of money in foreign currencies to the accounts of Company B, registered in an offshore jurisdiction, as payments "for patents".

The investigation carried out jointly with competent authorities revealed that Company A didn't carry out any real transactions involving patents.

Therefore, the reasons for transferring money to the accounts of Company B were fictitious and were in fact linked to money laundering.

Fig. 2.2.4[2].



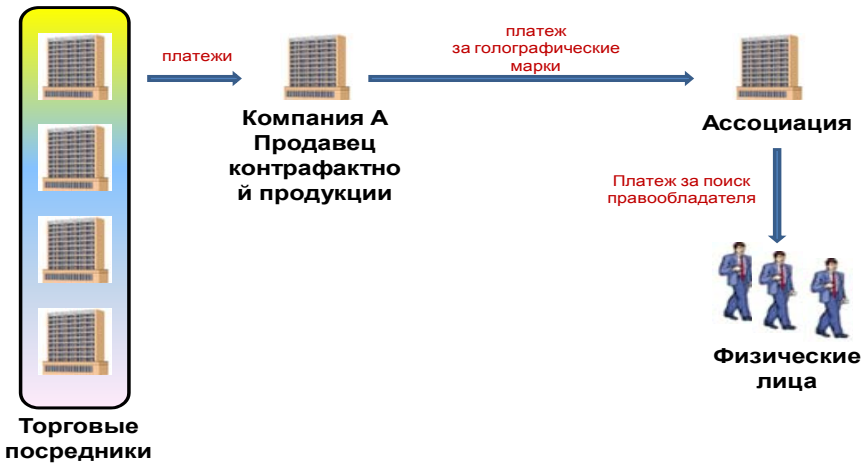
[2] **Торговые посредники** – ***Intermediaries***
Платежи за услуги на рынке объектов интеллектуальной собственности – *Payments for services in the intellectual property market*
Оффшорные юрисдикции – *Offshore jurisdictions*
За патенты - *For patents*
Компетентными органами установлено, что компания «А» не осуществляла реальных сделок с патентами - *Competent authorities revealed that the Company "A" did not carry out any real transactions involving patents*

2.2.5. A money laundering scheme involving the purchase of hologram marks

Traders in counterfeit goods send a list of audio/visual products they purchased to the Association they signed a licensing agreement with and receive from it protective hologram marks for their goods. After this, the traders in counterfeit goods claim that their products are authentic since they have received royalties as payment under the license agreement. This scheme allows traders to evade criminal liability for copyright infringement.

Under the terms of such license agreements, the Association accepts the responsibility for settlement of all possible property and other claims made by the holders of copyright and allied rights and third parties, and undertakes to cover the cost of legal representation in court. The funds received as royalties are either spent or legalized as write-offs related the cost of searching for copyright holder and then appropriated.

Fig. 2.2.6[3].



[3] Торговые посредники – ***Intermediaries***
Платежи – ***Payments***
Компания «А», продавец контрафактной продукции – ***Company "A", trader in counterfeit goods***
Платёж за голографические марки - *Payment for hologram marks*
Платёж за поиск правообладателя - *Payment to carry out search for copyright holder*
Физические лица – *Natural persons*

2.2.6. A money laundering scheme involving compensation claims

Sometimes fraudsters experience difficulties with making certain types of payments, especially to non-residents, due to the legal complexity involved in their execution and enhanced oversight from financial institutions and fiscal authorities.

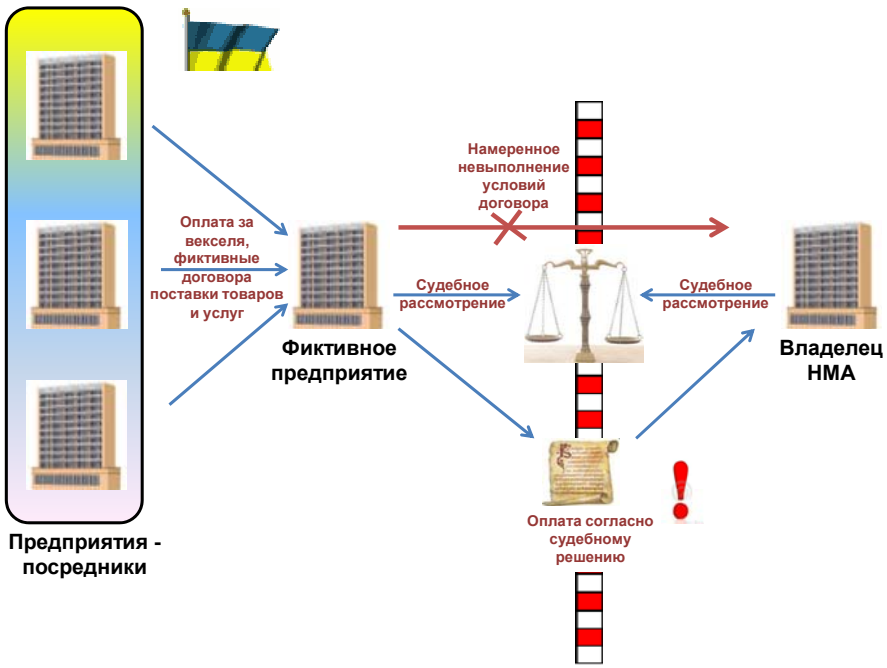
In such cases, a new element involving the use of IA is integrated into a money laundering scheme.

Two related companies knowingly enter into fictitious agreements for the purchase of or payment for the right to use IA.

One of them intentionally breaches the terms of the agreement so that the other can file a compensation claim in court.

Subsequently, following a court ruling in favor of compensation, the fraudsters are able to carry out the transactions they want since court rulings are subject to compulsory implementation.

Fig. 2.2.7[4].



[4] **Предприятия-посредники** - ***Intermediary***
Оплата векселя, фиктивные договора поставки товаров и услуг - *Payments for promissory notes, fictitious contracts for delivery of goods*
Фиктивное предприятие - ***Sham business***
Судебное рассмотрение - *Court proceedings*
Намеренное невыполнение условий договора - *Intentional breach of contractual terms*
Оплата согласно судебному решению - *Payment ordered by court*
Владелец НМА - ***IA owner***

2.2.7. A money laundering scheme involving assignment of claims

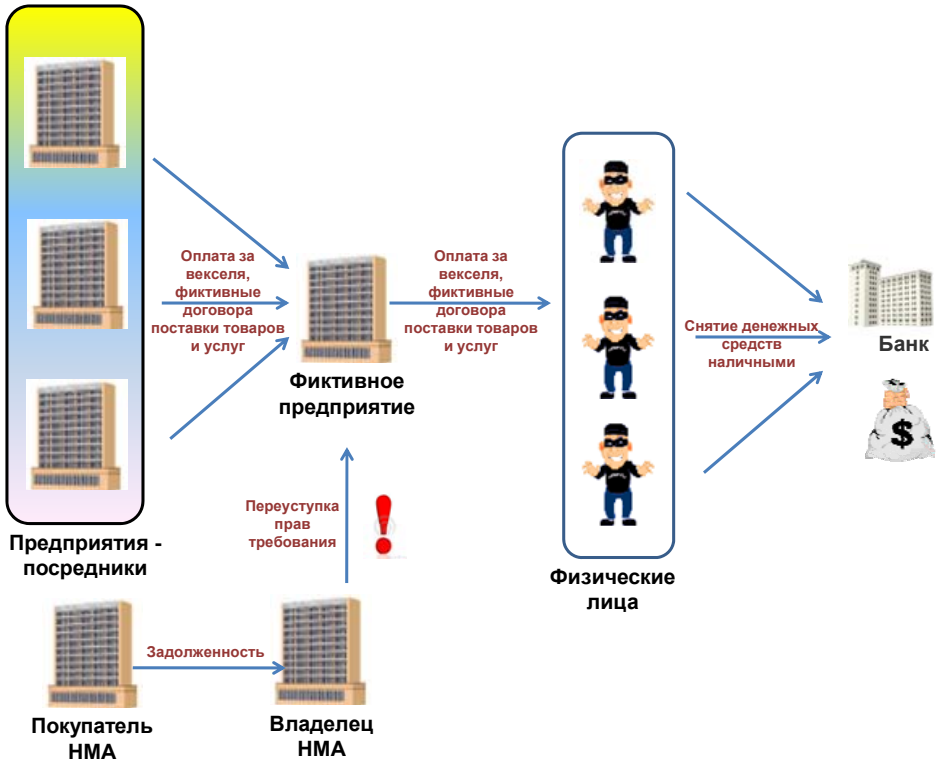
In their attempt to render the already known money laundering and terrorist financing schemes even more complicated, fraudsters use a variety of methods to conceal the true purpose of financial transactions.

For example, two related companies sign fictitious agreements for the purchase of or payment for the right to use IA.

Subsequently, when the payment date arrives, the beneficiary party assigns the right to the claim to a third party.

Ultimately, the funds were transferred to a company suspected of acting as a currency exchange center and cashed out.

Fig. 2.2.8[5].



It should be noted that in this case IA may not be listed as the payment purpose; instead, only the "under the claim assignment agreement" phrase may be used, which, of course, makes the task of a financial intermediary more difficult.

[5] **Предприятия-посредники** – ***Intermediary entities***
Покупатель НМА – ***IA buyer***
Владелец НМА – ***IA owner***
Оплата за векселя, фиктивные договоры, поставки товаров и услуг – *Payments for promissory notes, fictitious contracts for delivery of goods*
Задолженность – *Indebtedness*
Переуступка прав на требования - *Assignment of claims*
Фиктивное предприятие - *Sham business*
Физические лица - *Natural persons*
Снятие денежных средств наличными - *Cash withdrawals*
Банк - *Bank*

2.2.8. A money laundering scheme involving the purchase of promissory notes

Due to the subjectivity of pricing, IA can be used to create a different, more convenient mechanism for redistribution of financial resources.

For example, two related companies sign fictitious agreements for the purchase of or payment for the right to use IA.

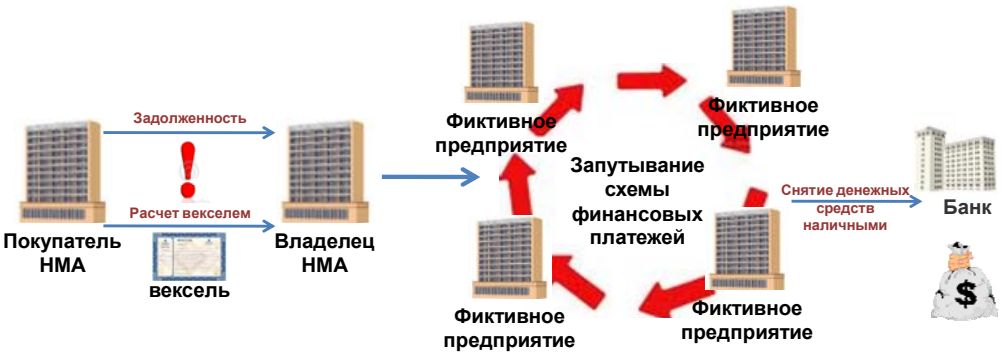
Subsequently, when the payment date arrives, the debtor company uses a promissory note to settle the debt.

As a rule, such promissory note comes with long maturity and is used by many intermediary companies.

Typically, such transactions are carried out with the ultimate goal of converting funds into cash or to conceal the payment pattern.

IA, in this situation, are unique for their ability to create a long-lasting (duration of the maturity period) indebtedness, i.e. a reason for issuing a promissory note.

Fig. 2.2.9[6].



[6] **Покупатель НМА** – ***IA buyer***
Задолженность – *Indebtedness*
Расчёт векселем – *Use of promissory note for payment*
Вексель - ***Promissory note***
Владелец НМА – ***IA owner***
Запутывание схемы финансовых платежей - *Payment pattern concealment*
Фиктивное предприятие - ***Sham business***
Физические лица - ***Natural persons***
Снятие денежных средств наличными - *Cash withdrawals*
Банк - ***Bank***

Some elements of this scheme may be repeated multiple times to add to the scheme complexity or as a mechanism for misleading law enforcement agencies conducting investigations.

3. Criteria for identifying suspicious transactions

Transactions involving IA carried out in countries participating in the typological study will, one way or another, be subject to anti-money laundering and terrorist financing supervision.

In particular, if a financial intermediary suspects a transaction to be linked to money laundering or terrorist financing, such institution must submit within a specified period a relevant report to the competent authority. The same is true with respect to IA-related transactions.

Based on the established practice, it's possible to single out the following groups of indicators of suspicious transactions that can be used to make an informed decision about whether a transactions with IA is linked to money laundering or not:

1. A suspicion about the client (registration details of an entity);
2. A suspicion about financial transactions and their nature;
3. A suspicion about documents confirming IA ownership.

1) A suspicion about the client (registration details of an entity) includes the following components;

- absence in the client's (legal entity) possession of any assets justifying the need for the use of IA;
- it's not possible to determine the physical location of the client (legal entity).

2) A suspicion about financial transactions and their nature includes the following components;

- IA (i.e. software, databases, stamps, etc.) represent the subject matter of an agreement;
- IA cost does not correspond to the real value, the client's financial ability or at odds with his normal business practice;
- recurrent nature of one-type transactions executed by the parties to the scheme;
- transactions are executed within the shortest possible time (often within a single day);
- financial transactions involving IA whose value cannot be determined;
- apparent discrepancy between the account turnover and sums of additional payments (taxes, pension fund deductions, etc.).

3) A suspicion about documents confirming IA ownership includes the following components:

- absence of documents confirming IA ownership;
- absence of any agreements confirming the transfer of ownership rights from one party to another as a result of a purchase or sale.

It should be noted that the above risk indicators may combine or evolve as a result of national specifics, domestic legislative framework, etc.

When dealing with suspicious transactions involving IA, special attention should be devoted to foreign trade transactions. In particular, suspicious are deemed transactions with non-residents registered in countries and areas offering preferential tax treatment, or when a non-resident's country of registration specified in the contract is different from the country of jurisdiction of the non-resident bank in which the non-resident's account is open.

It should be noted that the greatest risk is associated with international money transfers.

We should separately mention the criterion for suspicious transactions that applies to transactions involving import of the results of intellectual activities carried out without the simultaneous payment of value added tax.

Russia uses the following risk scale for IA-related transactions:

Intangible asset	**Risk level**		
	transactions between residents	transactions with non-residents	
		inbound transfers	outbound transfers
payment for the right to use property	low	average	average
payment for copyrights	average	high	high
payment for the right to use trademarks	average	high	high

4. Identification Practice

Identification of suspicious financial transactions related to IA may be carried out by financial intelligence units, law enforcement or other agencies responsible for monitoring the activities of entities during field inspections, operational activities, analysis of financial and other reports, studies of financial transactions, etc.

The procedure for analyzing financial transactions can be split into the following steps or stages:

- verification of submitted data;
- development of a working scenario;
- collection, evaluation and verification of additional information;
- building arguments.

Previous studies have shown that when dealing with IA-related transactions, it's necessary to consider the following transaction components:

- information about the IA owner;
- available documents confirming the ownership of IA.
- sums of money involved.

Information most often used when investigating cases related to IA:

Information type	Information source	Availability
Information about distribution channels for counterfeit products	Internet, public and governmental organizations	freely available or on request
Details of copyrights and patent registration	government organizations	on request
Information about the extent of damage	company representatives	on request

Evaluation is often carried out by contacting the manufacturer or an expert organization.

Therefore, when carrying out financial investigations, it's necessary to adjust the procedures used in such investigations regularly.