Conference Paper

The Impact of New Methods of Money Laundering on the Economy of the State

Karlov R. G.

National Research Nuclear University MEPhI (Moscow Engineering Physics Institute), Master Student, Institute of financial and economic security, Kashirskoe shosse 31, Moscow, 115409, Russia

Abstract

Modern information technology society is based on daily use of computer technology, communication networks, mobile communication and other technical facilities. Information technology is widely used in modern society not only in the workplace, is has entered almost all spheres of human life. The article presents new methods of laundering of proceeds of crime in the modern world. Today cybercrime is getting a huge scale, every day more and more people are trying to legalize their incomes in different ways by crime. This article shows the ways of solving the problem of money laundering in order to counteract effectively against the legalization of illegal income and reduce the level of crime in this sphere of activity.

Keywords: legalization (laundering) of incomes, combating, cybercrime, Internet

Corresponding Author:
Karlov R. G.
ruslan.karlov95@mail.ru

Received: 11 December 2017
Accepted: 20 January 2018
Published: 13 February 2018

Publishing services provided by Knowledge E

Selection and Peer-review under the responsibility of the FinTech and RegTech: Possibilities, Threats and Risks of Financial Technologies Conference Committee.

1. Introduction

Nowadays, criminals try to find new methods of money laundering in order to hide illegal source of income, thus they strongly influence the economic development of the state. The process of legalization of incomes is of great importance, because it allows criminals to use the profits obtained illegally without revealing its source. There are very many channels of profit by crime: illegal arms sales, smuggling and the activities of organized crime including for example drug trafficking and prostitution.

The spread of new information technologies gives extensive application of computer technology and communications, automation and optimization of processes in all sectors of life, put together by the intertwining of the boundaries of the state of the economies and infrastructures. A single global information space has been created in which everyone can have an access to information anywhere in the world, to manage their assets, enter into agreements without any personal contact. On the other hand, the information space becomes a place and an instrument of a crime. The crime did

not require prior "processing client" and personal contact with the victim. A computer and access to information and communication systems are the main tools of a criminal, where he is using illegal technical means and computer viruses gets full access to Bank accounts, databases and automated control systems.

Cybercrime becomes global. In addition, new technologies allow criminals to be anonymous, and rapid enrichment causes people to be interested in this illegal activity. According to the data, about 40 percent of the world population use the Internet (about 2.5 billion people) and the number of Internet users is growing regularly. During next four years, about 1.5 billion people will have access to the Internet. The popularity of the Internet is evident because the user working in the information environment has many possibilities – 24 hours access to information; fast communication with other users, conducting trade, banking and exchange operations. [1]

In addition, while investigative actions it is difficult to detect, remove and record important information for using it as evidence. In comparison with other types of crime, offences in the sphere of legalization and laundering of the proceeds have distinctive features and significant profitability, which is a significant "advantage" of this type of offences.

Thus, today research on new schemes and methods of money laundering is relevant and necessary.

2. Materials and methods

2.1. Federal Baliffs Service

Recently it became known that one of the key links in the fraudulent chain was the Federal service of bailiffs. The essence of the scheme is that two legal entities, one of which, the plaintiff is a non-resident, requires you to repay the debt, and the other defendant from the Russian Federation, agreeing with his claim, through arbitration courts or through amicable agreements negotiate the recovery of debt. The courts make the decision about collecting of money from the account of the debtor and issued a writ of execution. A non-resident brings the paper in the FSSP, which begins enforcement proceedings. To the account of the FSSP, the funds are debited from the bank account of the debtor, and then transferred to a non-resident to his account in foreign bank. Finally, the money laundering occurs through the state structure without breaking the law. [2]

The FBS has no right to assess the court's decision, strictly fulfilling it. The banks are in the same situation, which required fulfilling the request of the Federal bailiff service of money transfer. The schema can be revealed at the initial stage at the level of the courts by testing the reasonableness of the recovery of funds. Typically, the amount of debt greatly exceeds the turnover of the firms and the firms themselves do not have any business activity. However, the courts do not possess power, so the transaction is completely clean. The only thing that banks can make is to report about operations to the competent authorities, according to 115-FZ "On counteraction to legalization (laundering) of incomes obtained in a criminal way, and terrorism financing" but they must fulfill the requirement of the FSSP.

Thus, only for 2016, 16 billion left the country and it is 10% of the total detected questionable transactions for the year. The recommendations of the Bank of Russia, February 6, 2017 to credit institutions is specified to provide bigger attention to client operations when receiving funds via a court order, and the ability to realize the right to refuse to carry out transactions provided for 115-FZ [3]. In addition, it is recommended to terminate the relationship with the client, who twice in a year trying to use a scheme of withdrawal of assets and legalization of illegally obtained income through the judicial scheme.

A similar method of using court decisions was used in 2010-2014 in "Moldovan" scheme of theft and withdrawal funds from Russia. An offshore company had concluded the fictitious contract of loan for large amounts, the surety on which had been made by the Russian company. Upon expiration of the contract, the debtor did not return the loan due to lack of funds, translating the requirement to the company - guarantor. Thus, a fictitious debt of Russian commercial structures to the company from Moldova on the territory of which subsequently passed was formed and a Russian company adjudicated the litigation on the loan repayment. In the framework of the "Moldovan" scheme over $ 20 billion from Russia were withdrawn.

2.2. Online-casino

One of the most common ways of money laundering is the money laundering in a casino. Money are easy put into circulation either in the "win" (in collusion with the owners of the site), either in the revenue of the casino. Now this method is in a new form of online casino there is no need to enter cash in the cash register, you can replenish the balance via the Internet, terminal or bank.

The server for the website is established outside the Russian Federation and becomes uncontrolled by the Russian authorities. The main venues of advertising such sites is illegal online-cinemas, in which before watching the movie an online casino is advertising. Part of such ads is placed in social networks Vkontakte and Instagram. The administration of the social networks fight against such publications, but their efforts are not enough.

2.3. Social network as a Laundry for illegal money

A significant part of the population use social networks such as WhatsApp and Telegram, where security and encryption of connections is in a priority. After a history with leakedge of documents about wiretaps in different countries under the CIA, the number of users is growing exponentially. In addition to ordinary users, the attackers also find the advantages in using of encryption. For example, ISIS (banned in Russia as a terrorist organization) creates channels in the Telegram, through which recruits new members. Nowadays, the network administration blocks them at the request of security services. Nevertheless, in 2016 channels and bots, which offered a variety of services and products with huge discounts began to appear. They act according to the following scheme: the user makes a selection from the offered goods and services, after that the bot shows him a set of providers of the discounts with feedback of the clients to convince that the system really works. Selecting the option, the client continues to communicate directly with the seller on his channel, without any guarantees, but seller's reputation. The owners of the bots plan to include a service guarantee, where you can secure your order for a special fee.

Such best offers appear because of the need to launder money from stolen cards and e-wallets. Shadow entrepreneurs buy the product for the full prize and then resell at a lower price. Losing part of the money, they launder money practically imperceptible to the intelligence services. Because of small "crushing amounts "and of encoded social network it is almost impossible tracking the attacker as to prove his involvement in money laundering.

In addition to stolen cards, the attackers also use the promotional codes that are bought on the black market or get them via other people's bank and SIM cards thus getting discounts on goods and services. For Example, Yandex.Taxi gives a discount of 500 rubles on the first trip, and shady businessmen use it, when they offer short trips [4].

2.4. Cryptocurrency

The emergence of the term "cryptocurrency" is closely connected with the emergence of Bitcoin payment system. Cryptocurrency is a digital counting unit or the newest generation of currency, the main novelty of which consists in that it exists only in the virtual Internet and has no physical equivalent in the form of coins and banknotes. Later, the development of competitors: Ethereum, Ripple, Litecoin, Ethereum Classic and others appeared as shown in table 4 [5].

Bitcoin is a realization of a direct payment over the Internet. However, the attitude towards cryptocurrencies in modern world is ambiguous. The main danger of cryptocurrencies lies in anonymity, which can be used in fraudulent schemes, the financing of terrorism and drug trafficking. For example, in anonymous trading website Silk Road (Silk Road) where illegal goods are mostly sold, payment is made through Bitcoin. There are also a drawbacks of cryptocurrencies that is the demand for crypto currencies may lead to lower demand for the national currency, weakened the banking system, destabilizing the economy and, as a consequence, reduction of state intervention in the economy and currency regulation.

Cryptocurrencies can enhance liberalization of the world economy, as it is the first step to a free economy without barriers and protectionism. However, for companies which main goal is to legalize their income, terrorist organizations with cryptocurrencies have greater potential. Thanks to cryptocurrencies, economics of terrorism can be completely independent of the legal economic structures. It already has a small relationship with the legal economy. Some terrorist organizations control or provide the drug production, the proceeds from the sale of which are used to finance activities. It is also known that ISIL sells oil of the occupied territories on the market and only this source of income brings the group about $ 200 million. Terrorists can already meet the needs in education, carried out in special camps, etc.

3. Results

To date, the laundering of funds greatly affects the economy of the state and on business. International Monetary Fund points out several factors: the legalization of money affects major changes in the demand for money, distrust of banks, "infecting" effect on legitimate financial transactions, the volatility of international capital flows and exchange rates due to unanticipated transfers of foreign assets. Criminals are increasingly trying to find new methods of money laundering.

Many scientists tried to estimate the volume of money laundering on a global scale. The model developed by John Walker, head of the Australian division for the analysis of criminal activity is of great interest, because it allows estimating the volume of money laundering in the context of different countries, as well as the direction of the legalized income funds [6]. The United States is in the first place by volume of laundered funds is (46.3 per cent of the total). Russia is on the third position with 5.2 % for laundering in the world, as shown in table 1. The total level of money laundering around the world increased from 2.85 (1998) to 3.93 trillion (2011). Moreover, an essential part in the global money laundering accounts for the City of London and Wall Street. According to the Walker's model, the direction of legalization of incomes differs from their sources. The US still ranks the first place with data of 18.9% of the total. The second position is the Cayman Islands (4,9%), followed by Russia (4,2%), Italy (3,7%).

Table 1: Data on money laundering in the world (2011).

Позиция	Страна происхождения	Сумма (в млрд долл. США / год)	Процент от общей суммы
1	США	1,821.914	46,3
2	Италия	207.074	5,3
3	Российская Федерация	203.118	5,2
4	Китай	181.277	4,6
5	Германия	176.952	4,5
6	Франция	172.152	4,4
7	Румыния	159.507	4,1
8	Канада	113.676	2,9
9	Великобритания	94.861	2,4
10	Гонконг	86.741	2,2

Table 2: Data for the areas of money laundering in the world (2011).

Позиция	Страна направления легализации	Сумма (в млрд долл. США / год)	Процент от общей суммы
1	США	742.640	18,9
2	Каймановы острова	190.894	4,9
3	Российская Федерация	166.280	4,2
4	Италия	145.849	3,7
5	Китай	130.722	3,3
6	Румыния	123.641	3,1
7	Канада	117.913	3,0
8	Ватикан	111.222	2,8
9	Люксембург	108.286	2,8
10	Франция	94.490	2,4

Table 3: Correlation between the laundered funds and the rate of growth of real GDP (2011).

Страна	Темпы роста реального ВВП,%	Отмытые деньги /ВВП
США	1,10	3,90
Российская Федерация	6,00	3,40
Румыния	7,10	3,10
Болгария	6,00	2,90
Испания	1,20	2,80
Кипр	3,70	2,20
Германия	1,30	2,20
Швейцарская Конфедерация	1,60	2,10
Франция	0,40	2,10
Греция	2,90	1,90
Нидерланды	2,10	1,70
Австрия	1,80	1,70
Великобритания	0,70	1,60
Люксембург	0,90	1,20

Table 4: The Most popular cryptocurrency by market capitalization (November 2017).

Name of cryptocurrency	Market capitalization	Price
Bitcoin	$118 396 094 044	$7101.52
Ethereum	$30 343 693 662	$317.34
Bitcoin Cash	$10 552 653 322	$629.13
Ripple	$8 310 058 468	$0.215669
Litecoin	$3 335 640 167	$62.06
Dash	$2 460 543 728	$320.47
NEO	$2 117 290 500	$32.57

Significant amounts of localizable funds require the study of how the laundering happens in Russia. There are more than 120 typologies of laundering of money applicable in Russia. Laundering often occurs through front companies ("one-day firms"). In most cases (60%) for this cash, securities – 12% of all case, precious metals and precious stones – 6%, real estate and land – 4% are used. If to argue about the relationship between the laundered funds and the rate of growth of real GDP, we see in table 3 that the USA takes the 1st place with a growth rate of real GDP of 1.10%, Russia takes the 2nd place (6%), Romania occupies the 3rd place (7%).[7]

If the country has growing economic potential and developing financial centers, but there is no supervision, they are very vulnerable, because stable financial centers

introduce effective measures to combat money laundering. It could also be added that in a situation with a damaged reputation of financial institutions, money laundering negatively affects the foreign investments. For example, the Bank of Russia announced a substantial increase in the outflow of capital from Russia in January-April 2017. According to the regulator, capital exports made by the private sector during this period amounted to $21 billion, more than double fold the figure for the first four months of the previous year ($9.8 billion). [8]

4. Discussion

To detect and prevent new schemes, such as online casino, cryptocurrency, FSSP, social networks, it is necessary to attract Rosfinmonitoring, the Central Bank, which have the necessary experience and knowledge in this area. When revealing facts of fictitious transactions on the subject of the laundering of proceeds of crime, the scheme will be stopped at the initial stage. In addition, the court should have the right to carry out checks on the subject of the fictitious nature of the claim and further transfer of data to Rosfinmonitoring and to the Central Bank for making decision about the fictitious nature of the transaction and the suspension of the judicial process.

Strengthening of state propaganda with a warning about playing on the online sites can help to solve the problem. To prohibit the use of such sites is impossible, but the duty of the state is to warn citizens about the possible loss of money when using the sites. Of course, Roskomnadzor is blocking online casinos, but the cost of opening them is extremely small, due to this, these measures are ineffective, as after site closure occurs another.

Experts unambiguously assess the activities of the owners of the channels discounts as a criminal one. Not only Russians, whose credit cards and electronic wallets were stolen, can suffer from it, but buyers of services in the Telegram.

The lawyer Alexey Gurov, from the Bar of Moscow "Barshchevsky and partners" explains that users of Telegram that sell goods, purchased on a stolen credit cards, can be brought under article 159.6 of the criminal code "Fraud in the sphere of computer information" (till ten years of imprisonment). The person who buys goods or services may be recognized as a partner. In this case, the buyer of discounts will also expect a criminal punishment up to deprivation of liberty, says Gurov. The punishment for a partner determines the court.

Partner of the law Bureau "Zamoskvorechye" Dmitry Shevchenko said that, according to this article and article 159.3 of the criminal code "Fraud with the use of payment

cards", the swindler can be deprived of liberty for a term up to ten years with fine in amount of 1 million rubles or of a wage of a convicted person for a period up to three years. Fraud with coupons are also fraught with criminal prosecution under the article 165 of the criminal code "Causing damage to property by deception or abuse of trust" (to five years of imprisonment). In this case, the buyer of discounts, is likely to avoid accusations of complicity, said Gurov.

Telegram messenger also should not have legal effects for the actions of the sellers of discounts, though the executive authorities have the right for blocking the channels through which offenders pass on their messages, and with the appropriate authorization to disclose the operator's information about the criminals, says Shevchenko.

However, the head of law practice of the project "Roskomsvoboda" Sarkis Darbinyan notes that the detection of cases of money laundering in social networks is rather low. To investigate such crimes can be difficult due to the layered protection of anonymity, but also because of the difficulty to establish the fraud in the case of trade, based on promo coupons, sums up the expert.

In order to counter money laundering, all states are exchanging information on persons and organizations engaged in such activities. In accordance with Federal law No. 115-FZ "On counteraction to legalization (laundering) of incomes obtained in a criminal way and financing of terrorism" published in open access List of organizations and physical persons in who are related to extremist activities or terrorism. In addition, the Russian Federation had concluded bilateral and multilateral agreements on the exchange of information about the channels, methods and subjects of financing of terrorism.

5. Conclusion

Currently, a large part of classic business removes into the virtual sphere; the rapid development of the Internet is explained by this.

If you compare the "traditional" money laundering and cyber laundering, the second is based on the use of different types and providers of money services. For example, they are the provision of cash withdrawals, bank transfers, and e-money. As a rule, the chain stops at transactions where cash had been used carried out by "money mules", where you should use the traditional payment system. If the billing service includes online payments, the funds can be transferred to the e-mail anonymously and sent to another state. Identifying and monitoring of illegal cash flows is considered to be quite a challenge for the law enforcement agencies.

In this regard, an effective counteraction to legalization of illegal revenues and a reduction in the level of crime in this environment is possible thanks to the prompt identification of financial actions that can be associated with the laundering of money acquired in the field of cybercrime, effective international cooperation and cooperation between the private and the public sector.

Acknowledgements

This work was supported by Competitiveness Growth Program of the Federal Autonomous Educational Institution of Higher Education National Research Nuclear University MEPhI (Moscow Engineering Physics Institute).

References

[1] The Eurasian group on combating money laundering and financing of terrorism, the typological research project on the topic "Cybercrime and money laundering"

[2] The scheme imposed a penalty [Electronic resource]. URL: https://www.kommersant.ru/doc/3208167

[3] The Central Bank has instructed banks ways of dealing with a new money-laundering scheme [Electronic resource]. URL: http://www.rbc.ru/finances/07/02/2017/5898c55b9a7947265d4eb0c3

[4] Laundry discount: as the Telegram used for money laundering [Electronic resource]. URL: http://www.rbc.ru/money/10/03/2017/58c2d2a89a7947ef7749d2d2

[5] CryptoCurrency Market Capitalizations [E-resource]. URL: https://coinmarketcap.com/

[6] Smith D. Black Money: The Business of Money Laundering [Electronic resource]. URL: https://economywatch.com/economy-business-and-finance-news/black-money-the-business-of-money-laundering.08-06.html

[7] Stancu, I., Rece, D. The Relationship between Economic Growth and Money Laundering – a Linear Regression Model // Theoretical and Applied Economics, p. 4-5.

[8] The outflow of capital from Russia in January-April 2017 has more than doubled [Electronic resource]. URL: http://www.rbc.ru/rbcfreenews/5915bc8a9a7947477142oa4b