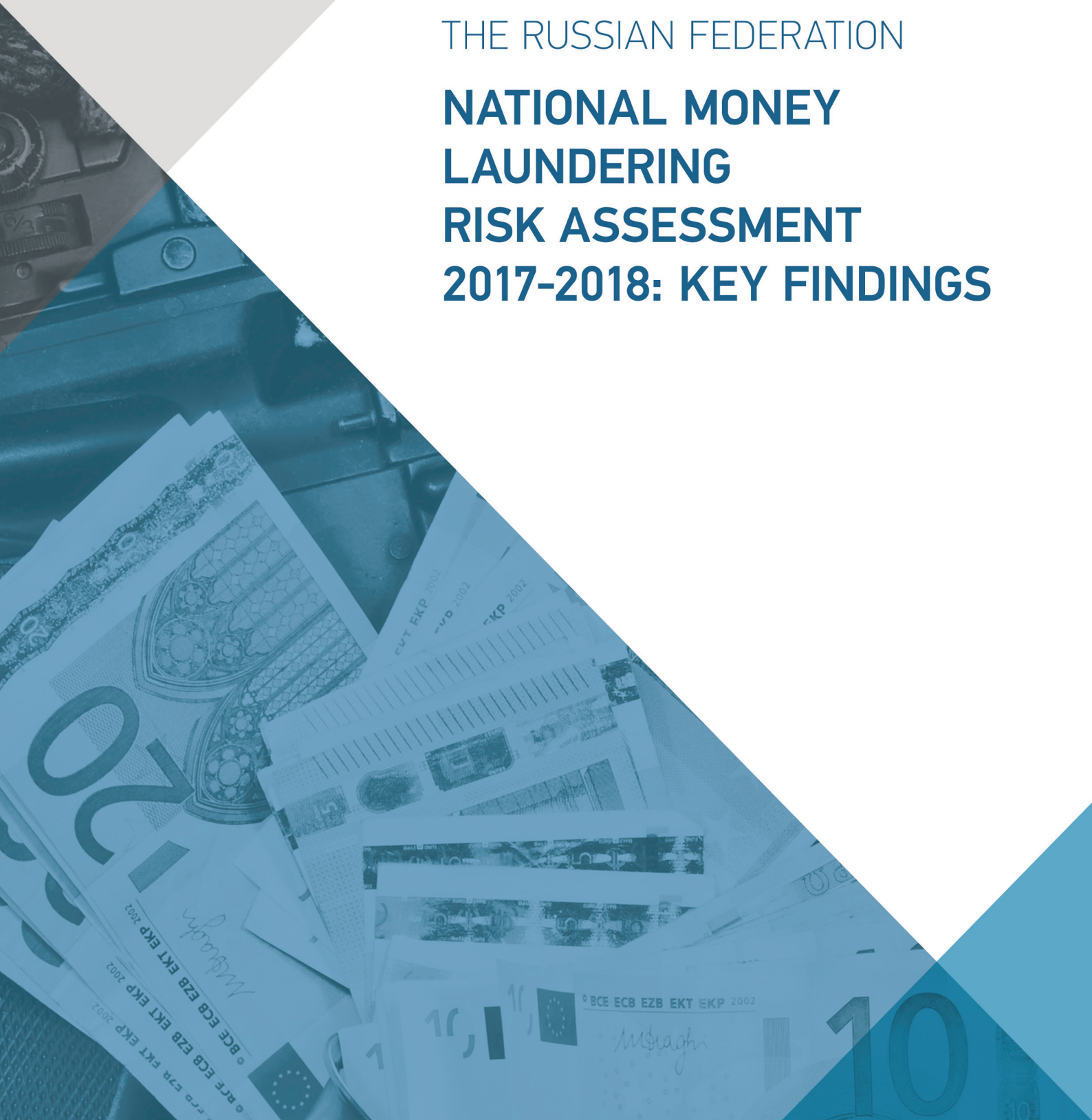
Public Report

FEDERAL FINANCIAL MONITORING SERVICE

THE RUSSIAN FEDERATION

NATIONAL MONEY LAUNDERING RISK ASSESSMENT 2017-2018: KEY FINDINGS



CONTENTS

The current English translation may contain some typos or inaccuracies which will be corrected later on.

ANNOTATION

In accordance with the FATF Recommendations and the Methodology, countries should continuously assess the risks of money laundering (ML) and terrorist financing (TF) with the aim of creating an adequate understanding at the national level of risks and threats to the financial system and the economy as well as the negative consequences that these acts pose. Countries should also develop adequate mitigating measures.

This document is a public version of the report on the national ML risk assessment (ML NRA). The Report contains the key outcomes of the assessment.

The results of the ML NRA are to be brought to the attention of all participants of the AML/CFT system (state bodies and the private sector) and are to be further used both in the practical aspect of applying risk-based approach and as contextual information in subsequent national risk assessments.

The outcomes of the ML NRA should be reflected: a) in sectoral risk assessments of supervisory bodies that assess ML risks in their respective sectors; b) in the internal control programs of the subjects of the Federal Law of 07.08.2001 №115-FZ "On Counteracting the Legalization (Laundering) of criminal proceeds and the Financing of Terrorism" (the AML/CFT Law), when developing risk management policy and in practical work when conducting risk assessment of customers, products, services, delivery channels, etc.

The outcomes of the ML NRA will be posted on the official website of Rosfinmonitoring.

LIST OF ABBREVIATIONS

GDP	Gross Domestic Product
FEA	Foreign economic activity
FSAP	Financial Sector Assessment Programme
PMPS	Precious metals and precious stones
IMF	International Monetary Fund
OCG	Organized criminal group
CSO	Shanghai Cooperation Organisation
CSTO	Collective Security Treaty Organisations
LEAs	Law enforcement agencies
KYC	Know Your Customer
MLA	Mutual legal assistance
FIU	Financial Intelligence Unit
CIS	Commonwealth of Independent States
STR	Suspicious transaction report
DNFBPs	Designated non-financial businesses and professions
EMP	Electronic means of payment
VAT	Value added tax

INTRODUCTION: OBJECTIVES AND TERMINOLOGY

The goals of the ML NRA are:

- Identification of the most frequently used methods of laundering criminal proceeds;
- Identification of weaknesses in the national AML system;
- Formation of a uniform understanding of risks among all participants of the AML system;
- Developing concrete measures and efficient allocation of resources to mitigate identified risks.

The following basic terms are used in the ML NRA:

National AML/CFT system	The composition of public authorities and other state bodies and organizations implementing state AML/CFT policy in cooperation with financial institutions and DNFBPs that carry out transactions with money or other assets, as well as the composition of instruments of organizational, coordinating, analytical, operational, regulatory and information nature that they have in possession.
National risk assessment of money laundering (ML NRA)	Activities of participants of the national AML/CFT system with the involvement of financial institutions and DNFBPs engaged in transactions with money or other property to identify and (or) prevent threats and vulnerabilities arising as a result of ML, to develop measures to counter them, as well as to prevent or minimize negative consequences.

ML threat	A person or a group, object or activity, which can potentially cause harm (to state, society, economy, etc.), i.e. criminals and persons supporting them, their money or other property, as well as their former, current and future ML activity.
Vulnerability of the AML/CFT system	A set of deficiencies of institutional, regulatory, legal, technical and other nature that hamper activities of bodies and organizations composing national AML/CFT system, and capable at certain conditions of leading to implementation of a threat.
ML risk	A possibility to cause damage to financial system and economy as a whole by way of committing financial transactions (deals) in order to launder criminal proceeds due to realization of a threat and (or) presence of vulnerability.
Consequences for financial system and economy	Mean impact or harm which may be caused by ML risks, and include impact associated with this criminal activity on financial system and institutions, but also on the entire economy. Consequences are also reflected on population, specific groups of people, business environment or on national, or international interests, but also on reputation and attractiveness of financial sector of a country[1].

[1] *Taking into account the practical difficulties associated with the quantitative assessment of the consequences, this assessment focuses on identifying and analysing the threats and vulnerabilities associated with ML, based on the understanding that ML incidents are constantly leading to significant negative consequences.*

HIGH-RISK AREAS

High-risk areas - mean areas that are highly exposed to threats and that have certain vulnerabilities. The areas where proceeds-generating crimes and ML processes are most likely to occur. The high-risk areas are determined on analysis of various sources information:

National and supra-national strategic documents, statistical data on major predicate crimes, suspicion financial transactions (STRs), proactive financial investigations, law enforcement (LE) requests, requests from foreign financial investigation units (FIUs), results of supervisory checks and monitoring; completed ML criminal cases; results of sector-specific risk assessments; results of survey among experts from the private sector, law enforcement and oversight bodies; information in media and reports produced by international organizations.

Based on the analysis of the information given above the following high-risk areas have been identified:

- **The area of budget spending and taxes**
- **Corruption**
- **Financial sector**
- **Drug trafficking**

IDENTIFICATION OF THE KEY THREATS

THE SOURCES OF INFORMATION ABOUT THE THREATS:

The following sources of information were used to determine threats: strategic documents and policies on national and financial security, inter-ministerial plans and decisions, national crime statistics, financial investigation cases and completed ML criminal cases, STRs and strategic analysis of aggregated financial flows; requests from competent authorities, outcomes of survey among state authorities and the private sector, supra-national strategies and policies (CIS, SCO, CSTO, etc.), the outcomes of the previous FATF and the 2016 IMF FSAP assessments.

Based on the analysis of the information provided above the following key threats have been identified:

Budget spending and taxes: fraud, misappropriation and embezzlement of public funds and assets. Also, tax crimes, in particular, VAT fraud and tax evasion by legal persons.

Corruption: corruption related crimes mostly committed by state employees (also, by employees of commercial and other organizations, including state corporations, entrepreneurs). This relates to: abuse of power, obtaining and giving bribes, mediation in bribery, commercial bribery, etc.

Financial sector: financial fraud with loans, assets allocated on bank accounts[2], deliberate or fictitious bankruptcy of financial institutions. Persons bearing a threat are: persons involved in fraudulent activities, dishonest management and owners of financial organizations.

Drug trafficking: large scale production of opiates in Afghanistan and their consequent trafficking including through the territory of Russia. Underground production of synthetic drugs within Russia as well as trafficking of synthetic drugs from neighbouring countries. The threat is posed by the activity of organized criminal groups and communities.

[2] Including fraud using electronic means of payment ("cyber fraud") - stealing someone else's property or acquiring the right to someone else's property by deception or abuse of trust, including taking possession of another's property or property rights by blocking, removing, modifying or otherwise influencing the means of storage, transfer or processing of electronic data, or information and telecommunications networks (Article 159-3 of the Criminal Code of the Russian Federation).

IDENTIFICATION OF THE KEY VULNERABILITIES

THE SOURCES OF INFORMATION ABOUT THE VULNERABILITIES:

The following sources of information were used to determine threats: strategic documents and policies on national and financial security, inter-ministerial plans and decisions, national crime statistics, financial investigation cases and finished ML criminal cases, STRs and strategic analysis of aggregated financial flows; requests from competent authorities, outcomes of survey among state authorities and the private sector, supra-national strategies and policies (CIS, SCO, CSTO, etc.) the outcomes of the previous FATF and the 2016 IMF FSAP assessments.

Based on the analysis of the information provided above the following key vulnerabilities have been identified:

- presence of a significant share of informal (shadow) economy;
- a relatively high level of cash circulation in the economy;
- the use of shell/front companies for ML purposes;
- concealment of illegal assets abroad;
- provision of risky financial services by some financial institutions;
- shortcomings in the existing legislation concerning measures preventing suspicious capital flight and cash transactions;
- the absence of state regulation and control on issuance and circulation of virtual currencies;
- shortcomings in the legislation governing the state procurement procedures (corruption links between public officials and contractors);
- lengthy consideration of requests for mutual legal assistance (MLA) from competent authorities of certain countries and difficulties in obtaining such assistance, as well as the information about beneficial ownership;
- insufficient awareness about ML risks and threats within some DNFBPs.

RISK ASSESSMENT

BRIEF METHODOLOGY DESCRIPTION

In this section, a final understanding of the national ML risks has been formed and evaluated based on the level of the identified threats and vulnerabilities. The risk assessment was carried out by rating the risks on the basis of statistical data, the results of the survey of the AML/CFT experts, as well as other qualitative (strategies, policies, etc.) and quantitative information (see above).

HIGH RISK GROUP

RISK OF USING NOMINAL DOMESTIC LEGAL PERSONS (SHELL/FRONT COMPANIES) IN ML SCHEMES

Decreasing

The use of nominal legal persons (shell/front companies) is common in ML schemes. This is indicated in particular by the results of financial investigation cases and completed criminal cases on predicate crimes and ML. Analysis of Rosfinmonitoring's database indicates a significant amount of money annually passing through accounts of legal persons with characteristics of shell/front companies. Front/shell companies are used by criminals in large part due to the possibility to conduct large-scale financial transactions to move the proceeds of crime, while hiding the ultimate beneficiaries of criminal schemes behind nominal founders and directors. Internet banking can be used to manage the accounts of such organizations. The risk is most typical for committing offenses in financial area, in the budgetary sphere, for the commission of corruption crimes, and to a

[3] For example, simplicity of setting up process, lack of liability of participants for the obligations of a company, the opportunity to establish theoretically an unlimited number of companies.

lesser extent affects the sphere of illicit drug trafficking. Vulnerability of legal persons is partly due to the peculiarities of the legislation regarding the setting up procedures[3]. As a result of the measures taken by the authorities over the recent years, however, the number of "shell/front companies" as of June 1, 2018 reduced to the historical minimum to around 300 thousand - this is approximately 7% of the total number of registered legal persons.

countries); b) countries with a favourable investment climate (in particular, countries in Western Europe, North America); c) countries with low transparency of the financial system, as well as with preferential taxation for non-residents (tax havens/offshore jurisdictions); d) countries from the "gray" and "black" lists of the FATF. There were examples of withdrawal of assets that have doubtful origin to South-East and Central Asia countries.

RISK OF USING FICTITIOUS FOREIGN ECONOMIC ACTIVITY IN ML SCHEMES (TRADE-BASED ML)

Decreasing

Schemes of withdrawal of funds that have a doubtful origin abroad are common and are mainly used to ensure the functioning of the informal ("shadow") economy ("gray" imports, evasion of tax and customs payments). At the same time, these schemes are also used to launder money abroad obtained from corruption, financial fraud, crimes with state funds. Channelled to foreign jurisdictions, criminal income is invested, as a rule, in residential and commercial real estate, legal businesses, luxury goods, and also stored on deposit and other accounts with foreign banks. To conceal the ultimate beneficiaries and financial assets, foreign legal persons and entities are used, usually registered in tax havens/offshore jurisdictions. The level of vulnerability is affected by:

- insufficient legislative measures preventing the use of fictitious/sham transactions and agreements;
- violations of legislation committed by shell/front companies.

The most risky destinations are: a) countries in Eastern Europe (the so-called "transit"

RISK OF USING NON-RESIDENT LEGAL PERSONS AND ENTITIES IN ML SCHEMES IN FOREIGN JURISDICTIONS

Decreasing

The use of foreign legal persons and entities (especially those registered in tax havens/offshore jurisdictions) is quite common in ML schemes committed abroad. The main vulnerability is the difficulty in obtaining reliable information about the beneficial owners of such companies and entities. Registration, as a rule, is carried out using front persons and legal entities in offshore jurisdictions. To conceal the ultimate beneficiaries and financial assets, complex corporate chains of interrelated legal persons and entities are used. Often, such jurisdictions do not have registers of beneficial owners or disclose such information reluctantly. There are cases of long consideration of requests sent to foreign countries for legal assistance and difficulties with obtaining such assistance from individual countries. The use of non-resident legal persons and entities is facilitated by the absence in the domestic legislation of the requirements for the repatriation of funds for contracts, according to which goods are purchased (sold) by residents from/to non-residents without their importation into the territory of the Russian Federation or export from the territory of the Russian Federation.

THE RISK OF USING CASH IN ML SCHEMES

 Decreasing

Cash is often used in ML schemes to conceal ill-gotten proceeds. In order to withdraw cash criminals use credit cards issued for front men, as well as corporate credit cards. The money received as a result of the commission of crimes (e.g. tax crimes or fraud) passes through a number of levels of nominal legal entities or electronic means of payment and is withdrawn to bank cards for the subsequent withdrawal in cash.

The processes of "cashing" also ensure the functioning of the informal economy (payment of "gray" wages, undeclared income and tax evasion). A significant share of cash circulation in the economy (although, the level of cash circulation is declining significantly over the recent years) is partly due to the economic model and context of the country. Anonymity of settlements using cash as well as the possibility to make large purchases for cash ensure the popularity of this method in committing crimes and, in addition, complicate the investigation process.

RISK OF ABUSING ELECTRONIC MEANS OF PAYMENT FOR ML PURPOSES

Electronic means of payment (hereinafter - EMP) (electronic wallets and pre-paid cards) are used in payment for drugs and subsequent ML. Criminals abuse the existing legislative regulation of electronic money, in particular, the possibility of using non-personalized (anonymous) EMPs (owned by individuals) to commit illegal financial transactions by transferring funds from one anonymous electronic wallet to another[4]. There have been cases of using EMPs registered in the name of the so-called "drops", i.e. persons who are not aware of the nature of the use of these tools.

RISK OF USING VIRTUAL CURRENCIES (SUCH AS BITCOIN, ETC.) IN ML SCHEMES

 Increasing

The cases of using virtual currencies in committing crimes in the sphere of economy on the territory of the Russian Federation were not recorded. At the same time, crypto-currencies can be used at various stages of drug trafficking, including purchase/sale of drugs, ML of criminal proceeds and distribution of funds between organized criminal groups, as well as payment of rewards to distributors, drug couriers and the workers of drug labs. In 2017, the facts of using Bitcoin in the financial structure of illicit drug trafficking were recorded in 23 regions of the Russian Federation. Anonymity of settlements using crypto currency can lead to a potential growth of popularity of this method in the commission of crimes, and in addition, complicates the investigation process.

[4] At the moment, the Ministry of Finance of Russia, with the participation of the Bank of Russia and Rosfinmonitoring, has prepared legislative initiatives aimed at minimizing the risks (including in terms of identification) of using non-personalized ("anonymous") EMPs in order to conduct suspicious transactions, and reducing the attractiveness of such EMPs for ML/FT).

THE RISK OF PARTICIPATION OF INDIVIDUALS (INTERMEDIARIES) ASSOCIATED WITH PUBLIC OFFICIALS IN ML SCHEMES


Decreasing

This risk is most typical for laundering proceeds obtained as a result of the theft of budget funds, the commission of corruption crimes. Various forms of association with public officials (colleagues, relatives, friends, former fellow students, etc.) are used. There are cases when state contracts were concluded with companies (executors, contractors, developers) owners and directors of which are persons associated with public officials. This facilitates the process of theft and ML through a chain of nominees, nominal and controlled legal persons. The following factors affect the level of vulnerability:

- large amounts of funding for infrastructure projects which complicates the process of monitoring the expenditure of allocated funds;
- long timeframes for the implementation of large state projects complicate control over the allocated funds;
- public-private partnership in large projects opens the access for private companies to budgetary funds;
- shortcomings in the legislation governing the state procurement procedures (conflict of interests and corruption links between public officials and contractors).

INCREASED RISK GROUP

THE RISK OF ABUSING BANKS, MICRO-FINANCE COMPANIES AND CONSUMER CREDIT COOPERATIVES FOR ML PURPOSES


Decreasing

The banking sector as a whole is the most regulated and law-abiding in terms of compliance with the AML/CFT legislation. At the same time, for the banking sector, due to its dominant role in the structure of the financial sector, the universal nature and accessibility of financial services, there is a high level of threat from criminal elements - persons involved in fraudulent activities, corrupt officials, organized criminal groups, etc. The main vulnerability of the sector is the presence in it of individual financial organizations whose business can be to a certain extent focused on personal enrichment of their management and owners by way of carrying out high-risk financial services.

The vulnerability of micro-finance companies and consumer credit cooperatives is partly due to the relative simplicity of registration process (as compared to banking sector) and also the specifics of the sectors (the possibility to attract funds of legal persons and redistribute them among individuals). The Bank of Russia, in conjunction with LEAs, the Prosecutor General's Office and Rosfinmonitoring, is consistently engaged in withdrawing such financial institutions

from the financial market[5], in particular, reducing the number of "unreliable" and high-risk banks: from 150 in mid-2013 to 3-5 banks in 2017. As a result, a significant and consistent decrease in the volumes of suspicious financial transactions of clients of financial institutions has been achieved, in particular, with regard to suspicious cross-border and cash transactions. The measures taken over the recent years have significantly reduced the level of ML risk in the banking sector and in the sectors of micro-finance companies and consumer credit cooperatives.

RISK OF USING THE MARKET OF PRECIOUS METALS AND PRECIOUS STONES IN ML SCHEMES

The sector is characterized by an increased level of ML risk for a number of reasons. Vulnerability of the sector is due to the insufficient level of implementation of the AML legislation by participants in certain segments of the sector, as well as the need to improve the sanctioning measures and state control. There is an increased level of threat of committing typical predicate offenses in the sector - the use of illegal and partly legal ways to avoid paying taxes, including VAT, illegal mining of precious metal, illegal refining and smuggling of precious stones. Nevertheless, a set of measures that is being implemented in the sector should mitigate the existing risks to a large extent (see section on measures taken).

RISK OF USING MONEY TRANSFER SYSTEMS (MTS) IN ML SCHEMES

In spite of the fact that this method practically does not appear in the ML schemes from such predicate crimes as fraud, corruption, theft, etc., there are examples of using money transfer systems when making payments in small amounts for narcotics (mixing them with legal remittances from seasonal works in Russia). The main threat comes from representatives of illegal migration and ethnic organized crime groups (mainly from Central and Eastern Asia, Ukraine) involved in drug trafficking. The risk of using money transfer systems to pay for drugs and ML is to a certain extent mitigated by existing corporate and state control, since operators of such systems have the status of credit institutions and, as a rule, are part of banking groups.

RISK OF USING SECURITIES MARKET IN ML SCHEMES


Decreasing

One of the vulnerability factors of the securities market is the possibility of carrying out settlements using bearer bills of exchange (in particular, commodity bills) which makes it difficult to establish a connection between the buyer and the seller. Among other factors, there is an insufficient transparency in transactions with securities, in particular with the participation of depositories. The most vulnerable in terms of involvement in potential illegal activities are small companies working in this sector. Under the guise of transactions with securities, money that has doubtful origin can be transferred abroad. The measures taken by the Bank of Russia over the recent years made it possible to withdraw a number of dishonest participants from the market, reducing significantly the potential ML risks.

[5] *The system of monitoring and analysis of financial transactions was reformed, new algorithms for processing information were developed which made it possible to speed up the efficiency of identifying suspicious financial transactions, their suppression and reaction to their transformation. Joint work was organized with banks and non-credit financial institutions using elements of advisory supervision, applying preventive measures to those participants who "did not listen" to the recommendations of the Bank of Russia, and withdrawal from the financial market of supervised organizations that ignored the messages and instructions of the Bank of Russia).*

THE RISK OF CROSS-BORDER MOVEMENTS OF CURRENCY AND BEARER NEGOTIABLE INSTRUMENTS (BNIs) IN ML SCHEMES


Decreasing

False or non-declaring, as well as smuggling of currency and (or) BNIs, carries certain ML risks, largely due to: a) the existence of the extended customs border of the EEU; and b) the absence of a legal requirement for individuals to provide documents confirming the origin of currency and BNIs, when moving them across the customs border of the EEU. The risk is partially mitigated by the existing legislative restrictions and a high level of control over the movement of currency and BNIs. There are serious sanctioning measures for false or non-declaring, as well as for smuggling. Although, since 2015 there has been a trend towards an increase in the amount of currency that is being declared across the border, the amounts of illegally transferred currency and BNIs are declining.

MODERATE RISK GROUP

THE RISK OF USING THE INSURANCE SECTOR IN ML SCHEMES


Decreasing

In 2016-2017, the risks of using the insurance sector for illegal purposes were significantly reduced, largely due to the deprivation of licenses of a number of insurance companies that did not comply with the requirements of the Bank of Russia and (or) carried out suspicious financial transactions (transfer of funds that have suspicious origin abroad under the guise of "re-insurance"). The sector as a whole is characterized by a proper level of compliance with the AML/CFT Law and awareness of ML/FT risks and trends. No critical vulnerabilities have been recorded.

THE RISK OF USING REAL ESTATE SECTOR IN ML SCHEMES


Decreasing

The level of threat of potential use of the sector is estimated as increased. The facts of the acquisition of immovable property for criminal proceeds appear in the materials of criminal cases under articles 174, 174.1 of the Criminal Code of the Russian Federation. The main factor of vulnerability is high liquidity of real estate, relatively low transaction costs of its use for investment purposes. Another vulnerability factor is the absence of formal legal restrictions for purchasing real estate with cash. It should be noted, however, that with the development of financial services and electronic means of payment in recent years the volume of cash

transactions has been steadily declining. In addition, a significant share of the real estate market is formed through transactions with the use of mortgage lending[6]. In addition, all financial transactions with real estate in excess of 3 million roubles (approximately 47000 USD) are subject to mandatory threshold reporting to Rosfinmonitoring. A certain ML risk in the domestic real estate market relates to direct investment (without involvement of real estate agencies) in the construction field.

At the same time, the main risks of ML through the real estate sector are related to the investment of capital that has suspicious origin in commercial and residential real estate abroad. The risk, in particular, is due to the lack of transparency in the beneficial ownership structure of property owners acquired in foreign jurisdictions.

The real estate sector as a whole is characterized by a sufficiently proper level of involvement in the AML/CFT system and law-abiding behaviour. A feature of this business in the Russian Federation is that a real estate agent is not a mandatory party to the real estate transaction. In the domestic context, the sector is more focused on providing consulting services and information support. Typically, the real estate agent does not participate directly in the transaction, as well as in the settlements between the seller and the buyer. In addition, banks and notaries play an integral role in verifying customer data and the legality of transactions when performing transactions with real estate. In recent years, there has been a trend in the Russian Federation to replace the traditional services rendered by real estate agents in the selection of real estate objects for a client by alternative electronic systems in the Internet (for example, www.cian.ru, www.domofond.ru, etc.). A number of such services for the selection of real estate are organized by banking institutions to promote the mortgage products (for example, domclick.ru service from PJSC "Sberbank").

THE RISK OF ABUSING POSTAL REMITTANCES SERVICES IN ML SCHEMES


Decreasing

The risks of using the federal postal service for the purpose of making suspicious cash transactions appeared in 2013-2014 as a result of increased control by the Bank of Russia in the banking sector. Following the application of supervisory measures, interdepartmental coordination and improvement of the organization of the internal control system within the framework of fulfilment of the AML/CFT obligations in 2015-2016, there has been a significant reduction in the number of suspicious transactions conducted through the Russian Post. At the same time, in 2017, attempts were made to re-use the services of the Russian Post to carry out suspicious financial transactions (in particular, through the mechanism for providing postal money transfers from companies to natural persons within the framework of contracts concluded between the Russian Post and companies. Natural persons subsequently receive postal money transfers in cash in post offices).

THE RISK OF ABUSING THE SERVICES OF NOTARIES FOR ML PURPOSES


Decreasing

The risk of abusing notaries for ML purposes today is estimated as moderate. The measures taken in 2017 by Rosfinmonitoring together with the Ministry of Justice of the Russian Federation and the Federal Notary Chamber allowed stopping the

[6] *Banks when providing customers mortgage products implement not only a standard set of KYC procedures, but also a detailed credit standing analysis using different scoring systems. Banking institutions carefully study real estate transactions for any indication of illegal activity including ML and in case of identifying such an indication submit a STR to Rosfinmonitoring and apply enhanced measures).*

emerging attempts to use the deposit accounts and the executive inscriptions of notaries for "cashing" money. At the same time, there have been cases identified where on the basis of formally legitimate executive inscriptions issued by notaries within civil litigation processes concerning debts collection from legal persons in favour of natural persons, suspicious cross-border transactions were carried out.

THE RISK OF ABUSING THE LEASING SECTOR FOR ML PURPOSES


Decreasing

The leasing market in Russia is dominated by companies with state participation, as well as by leasing companies that are part of large financial groups. In this sector, a high level of corporate control is supplemented by a system of state financial control which is reflected in a proper level of the AML/CFT compliance, a low level of criminal activities within the sector and rare examples of abuse of leasing companies for ML purposes. The potential ML risks are rather inherent in the small and micro business segment which accounts for no more than 3% of the market. One of the vulnerabilities for the sector is the relatively easy access to the market mainly due to the absence of restrictions on the minimum amount of capital for its participants. In addition, a high level of dependence of leasing companies on parent financial institutions can be noted as a potential vulnerability. If a parent company is involved in a high-risk activity the corresponding ML risks may potentially transform into a subsidiary leasing company.

The sector is generally characterized by a high level of compliance with the AML/CFT Law and a proper awareness about the ML/TF risks. At the same time, the scale of the sector and the presence of vulnerabilities indicated above, which are mainly of an institutional nature, form a moderate level of ML risk in it.

THE RISK OF ABUSING THE SERVICES OF MOBILE OPERATORS FOR ML PURPOSES

The sector of mobile communication operators is characterized generally by a sufficient level of compliance with the AML/CFT legislation. As part of supervisory inspections some violations of the anti-laundering legislation have been revealed that are more of a minor nature. There have been no proved cases of mobile phone operators being involved in ML activity. Nevertheless, there has been some suspicious activity identified recently indicating that the services of mobile phone operators could be abused in order to conduct high-risk transactions. The ultimate goal of these transactions appear to be the transfer of funds and their withdrawal into an uncontrolled cash turnover involving natural and legal persons that have characteristics of shell companies/ front men, presumably to conceal income from taxation.

THE RISK OF ABUSING PAWNSHOPS FOR ML PURPOSES


Decreasing

There are rare and isolated cases of pawnshops being involved in unlawful activities and ML schemes. Supervisory measures conducted by the Bank of Russia also do not reveal circumstances that indicate the existence of high or increased ML risks in pawnshop activities. The need to improve the procedure for admission of pawnshops to the financial market can be noted as a potentially vulnerability of the sector[7].

[7] *At the moment, the draft law "On Amendments to Certain Legislative Acts of the Russian Federation" has been drafted which provides for conducting checks by the Bank of Russia of the documents of a legal person intending to obtain the status of a pawnshop, including an assessment of compliance with the requirements for business reputation of management bodies and pawnshop founders (participants), that is, establishment of a procedure similar to the market entry procedure for microfinance organizations.*

THE RISK OF ABUSING OPERATORS THAT COLLECT PAYMENTS FOR ML PURPOSES

 Decreasing

There were cases of participation of payment and bank payment agents (subagents) in high-risk transactions involving sale of cash delivered by natural persons to payment terminals as payment for services and goods, in violation of the Federal Laws No. 103-FZ and No. 161-FZ. Under this scheme cash was transferred to a third-party - so-called "cash beneficiaries" who "paid" for the cash and in return transferred non-cash funds to the accounts of payment and bank payment agents (subagents), including through numerous transit transactions involving legal persons that have a low tax burden and other signs of fictitious activities.

LOW RISK GROUP

THE RISK OF ABUSING OTHER FINANCIAL SECTORS AND DNFBPS (MUTUAL INSURANCE COMPANIES, MUTUAL INVESTMENT FUNDS, INVESTMENT FUND MANAGEMENT COMPANIES, PRIVATE PENSION FUNDS, AUDITORS, LAWYERS, FACTORING, GAMBLING SECTOR, ADVOCATES, ACCOUNTANTS) FOR ML PURPOSES[8]

The results of sectoral ML risk assessments, the analysis of financial transactions, very rare cases of the sectors being abused for criminal purposes, a low percentage of violations of the AML/CFT Law, low estimated potential damage, etc. - all these factors when combined indicate a low level of risk for the sectors to be abused for ML purposes.

THE RISK OF USING INFORMAL MONEY TRANSFER SYSTEMS SUCH AS "HAWALA" FOR ML PURPOSES

No cases have been detected that would confirm that informal money transfer systems such as "Hawala" operate in the territory of the Russian Federation and can be used for ML purposes.

[8] Within the context of this document the term "accountants" refers to persons who conduct business activities in the field of providing accounting services.

MEASURES TAKEN/BEING TAKEN TO MITIGATE THE ML RISKS[9]

HIGH RISK GROUP

RISK OF USING NOMINAL DOMESTIC LEGAL PERSONS (SHELL/FRONT COMPANIES) FOR ML PURPOSES

The government authorities carry out a set of measures to eliminate shell/front companies: mechanisms have been introduced to prevent the registration of such companies and the use of dummy individuals for this purpose.

Preventative measures are actively applied in the form of a unified list of customers of financial institutions (Federal Law No. 424-FZ of December 30, 2015) in respect of which banks have made a decision:

- to refuse to conduct a transaction;
- to refuse to open a bank account;
- to terminate banking services contract due to ML/TF suspicions.

The unified list of clients mentioned above is formed by Rosfinmonitoring and transferred to the Bank of Russia for the purpose of subsequent use by financial institutions when assessing the level of risk of their customers.

The Federal Tax Service of Russia (FTS) conducts regular work (Federal Law No. 67-FZ of March 30, 2015) to verify the authenticity of the information contained in the Unified State Register of Legal Entities in order to prevent the registration and activity of companies created for unfair and illegal activities by providing inaccurate information during registration. Regular interaction is being made between the Federal Tax Service of Russia and financial institutions to take measures to terminate banking account contracts in case of suspicion of carrying out transactions on behalf of a shell/front company.

As a result of the measures applied, the number of "shell/front companies" as of June 1, 2018 reduced to the historical minimum to around 300 thousand - this is approximately 7.3% of the total number of registered legal persons. For comparison, in 2016 the number of such companies was estimated to be at around 1.6 million.

[9] The list of measures provided is not exhaustive.

The decrease in interest in the use of "shell/front companies" is also due to the introduction of an automated system for monitoring VAT reimbursement (ASK VAT-2) which allows to identify actions aimed at minimizing the difference between incoming and outgoing VAT because of shell companies and fictitious invoices. This system in real time compares information about purchases and sales, reveals discrepancies in VAT declarations and, therefore, various "shadow" schemes. As a result, for the first quarter of 2018, without audits with the help of this system, it was possible to additionally collect 12 billion rubles (around 200 million USD) into the federal budget, which is 1.8 times more than the same period of the previous year.

The effectiveness of criminal procedural mechanisms (*Federal Law No. 308-FZ of October 22, 2014*) in the sphere of combating economic crimes has been increased.

The Russian Federation has joined the multilateral agreement of the competent authorities on the automatic exchange of financial information, which will allow the Federal Tax Service of Russia, starting from September 2018, to obtain information on the financial accounts of the Russian taxpayers from the competent authorities of 74 (according to the information published on the OECD website as of 10.04.2018) foreign jurisdictions (including offshore jurisdictions).

Federal Law No. 215-FZ of June 23, 2016 introduced the obligation for legal persons to have information about their beneficial owners and to provide it at the request of authorized bodies and also established responsibility for violation of these requirements.

The Bank of Russia constantly communicates information on typologies and suspicious activity indicators involving shell/front companies to supervised institutions.

THE RISK OF USING FICTITIOUS FOREIGN ECONOMIC ACTIVITY ML IN SCHEMES (TRADE-BASED ML)

A legal requirement (*Federal Law No. 325-FZ of November 14, 2017*) is introduced for authorized banks to refuse to conduct cross-border transactions in foreign currency, if they contradict the requirements of the legislation on foreign currency regulation and control, or when a client provides documents that do not meet the established requirements.

A fixed amount of a fine for illegal cross-border currency transactions and for violation of the repatriation of monetary funds is established and can be imposed on responsible persons. Disqualification for repeated offenses of foreign currency control legislation is provided.

An obligation to repatriate funds to accounts in authorized banks that were previously transferred under loan agreements by residents to non-residents was established (*Federal Law No. 64-FZ of April 03, 2018*).

The Council of Europe Convention on Laundering, Detection, Seizure and Confiscation of the Proceeds from Crime and Financing of Terrorism has been ratified *(Federal Law No. 183-FZ of July 26, 2017*).

A draft federal law "On the Return of Assets that Were Derived from Corruption Offenses from Foreign Jurisdictions" has been developed.

A draft federal law "On Introducing Amendments to Certain Legislative Acts of the Russian Federation (regarding counteraction of unlawful financial transactions) is drafted. The draft law provides for giving the tax authorities, foreign currency control bodies and Rosfinmonitoring the right to apply to the arbitration court for participation in cases concerning transfer of funds to accounts of non-residents, and to make claims for invalidation of agreements and transactions if there are grounds to believe that transactions are or may be carried out for the purpose of committing an illegal financial activity.

In order to eliminate the gap in currency control legislation the Ministry of Finance of Russia has prepared a draft federal law "On Amendments to the Federal Law" On Currency Regulation and Currency Control" and "On Amending Article 15.25 of the Administrative Code of the Russian Federation". It imposes the obligation to repatriate funds under the contracts according to which goods are transferred within the territory of the Russian Federation, or outside the Russian Federation without their importation into the territory of the Russian Federation.

The Bank of Russia in order to reduce the ML/FT risk issues methodological recommendations for supervised entities concerning increased attention to certain types of transactions, specifically cross-border trade-based transactions.

As a result of the measures taken the volume of cross border suspicious financial transactions has been reduced more than 20 times from about 1.7 trillion rubles to 77 billion rubles in 2017.

THE RISK OF USING NON-RESIDENT LEGAL PERSONS AND ENTITIES IN ML SCHEMES IN FOREIGN JURISDICTIONS

An active work is going on with regard to the use by law enforcement agencies of information provided by Rosfinmonitoring that was obtained through international channels in order to identify and seize criminal assets that have been transferred abroad.

The obligation was introduced for financial institutions to apply identification procedures (KYC) to foreign legal entities (trusts, funds, partnerships) (*Federal Law No. 424-FZ of December 30, 2015*).

It is planned to prohibit by law (*draft law No. 599495-6*) the use of state support measures (including obtaining loans from a state-owned Vnesheconombank) to companies from Russia that are registered in offshore jurisdictions, as well as to require a legal person during the registration process with the tax authorities to provide information on the controlling persons - founders registered in Russia.

A set of measures have been taken to reduce the use of companies registered in offshore jurisdictions within the Russian economy (*Federal Law No. 376-FZ of November 24, 2014*).

Active measures are being taken to identify and return funds and other assets withdrawn from the country using non-resident legal persons and entities through civil litigation processes (e.g. the work that has been done by the state corporation Deposit Insurance Agency).

The government's policy to reduce the risks of using foreign legal persons and entities in the Russian Federation for illegal purposes resulted in a significant decrease in the amount of money withdrawn from the Russian Federation to offshore jurisdictions.

THE RISK OF USING CASH IN ML SCHEMES

The measures taken largely coincide with the measures specified under item 1 of the Increased Risk Group in relation to the risk of abuse of financial institutions.

The Bank of Russia in order to reduce the ML/FT risk issues methodological recommendations for supervised entities concerning increased attention to certain types of transactions, specifically cash-based transactions.

As a result of the actions taken the volume of cash related suspicious financial transactions has been reduced more than 3 times from about 1.2 trillion rubles to 326 billion rubles in 2017.

THE RISK OF ABUSE OF ELECTRONIC MEANS OF PAYMENT FOR ML PURPOSES

In order to further improve measures to combat cyber fraud and cyber theft, in April 2018 Federal Law No. 111-FZ of April 23, 2018 "On Amendments to the Criminal Code of the Russian Federation" was adopted. The law increased

the criminal liability for theft of someone else's property committed from a bank account, as well as electronic funds (imprisonment for up to 6 years). Amendments were made to the article of the Criminal Code of the Russian Federation providing for punishment for fraud using payment cards. A new qualifying attribute has been introduced - "from a bank account, as well as from electronic funds". Sanctions for fraud in the sphere of computer information have been adjusted. Instead of arrest for up to 4 months for fraudulent use of electronic means of payment, imprisonment for up to 3 years is provided. Threshold amounts of large and especially large amounts have been reduced in order to apply the relevant articles of the Criminal Code of the Russian Federation.

In addition, at the present time the State Duma of the Russian Federation is considering a bill (N 296412-7 "On Amendments to Certain Legislative Acts of the Russian Federation that concerns countering theft of funds in the sphere of electronic payments. Money transfer operators will be obliged to suspend execution of a transaction for up to 2 working days if they reveal that such transaction has signs of transfer of funds without the client's consent.

It is planned to legislatively prohibit the receipt by individuals of cash with the use of non-personalized electronic means of payment (*At present, in order to minimize the risks of using cash for ML/FT purposes, draft federal law No. 287876-7 is developed which is currently at the stage of preparation for consideration by the State Duma of the Russian Federation in the second reading. The draft Law imposes prohibition on receipt by individuals of cash with the use of prepaid cards which are non-personalized electronic means of payment*).

Rosfinmonitoring, together with experts from private sector entities is developing a model for the financial behaviour of a drug-trafficker in order to subsequently introduce the appropriate profile to the internal control systems of financial organizations.

THE RISK OF ABUSING VIRTUAL CURRENCIES (SUCH AS BITCOIN, ETC.) FOR ML PURPOSES

The draft law "On Digital Financial Assets", which defines the status of digital technologies used in the financial sphere and their basic concepts, including crypto-currencies, was developed (*The corresponding bill No. 419059-7 was submitted to the State Duma of the Federal Assembly of the Russian Federation on March 20, 2018. The provisions of the Bill regulate the procedure for issuing and exchanging crypto-currency and tokens for rub. and foreign currency, while providing that in order to reduce the risk of holders of digital financial assets and to ensure compliance with the requirements of the AML/CFT Law, such an exchange is possible only if appropriate identification procedures through the exchange operators of digital financial assets*).

This bill proposes a mechanism for regulating the circulation of crypto-currencies based on the standards of the Financial Action Task Force (FATF).

In 2014 and in 2017 press releases that notify individuals and legal persons about the risks of ML/FT associated with transactions with virtual currencies were published on the official website of the Bank of Russia.

The Ministry of Internal Affairs of Russia and Rosfinmonitoring within the Eurasian Group on Combating Money Laundering and Financing of Terrorism (EAG) conduct a typological study on identifying cross-border drug trafficking schemes and laundering of proceeds from illicit trafficking in narcotics using electronic payment systems and crypto-currencies. The study summarizes the data of law enforcement agencies and financial intelligence units of the EAG member countries on the methods of criminal financial settlements of this kind and models of legal regulation of the electronic payment system in various states.

THE RISK OF PARTICIPATION OF INDIVIDUALS (INTERMEDIARIES) ASSOCIATED WITH PUBLIC OFFICIALS IN ML SCHEMES

The effectiveness of control over the expenditure of budget funds by business entities that are of strategic importance for the defence industry and security of Russia, as well as organizations under their control has been increased: an institution of authorized banks has been established and additional administrative responsibility for offenses in this sphere has been enacted (*Federal Law No.159-FZ of June 29, 2015 and Federal Law No. 213-FZ of July 21, 2014*).

Enhanced financial monitoring is carried out over the use of budgetary funds at the placement and implementation stages of state defence orders and more broadly regarding state procurement and taxation. For these purposes, a special structural unit was set up in Rosfinmonitoring that deals with budgetary funds.

It is planned to further strengthen criminal and administrative responsibility in the sphere of state defence order (*Draft Federal Law No. 5198-7 and Draft Federal Law No. 4979-7*).

It is planned to establish a treasury control mechanism for funds provided on the basis of a state contract for the supply of goods, the performance of work, and the provision of services to ensure state and municipal needs.

The effectiveness of the system of public administration and control in areas subject to corruption risks has been improved (*Federal Law No.182-FZ of June 23, 2016*).

The criminal liability for corruption crimes is increased (*Federal Law No.324-FZ of July 3, 2016*):

- acts are recognized as crimes when money, securities or other property is transferred not to the official himself (a person performing administrative functions in a commercial or other organization), but at his instruction to another natural or legal person;
- criminal liability was introduced for mediation in commercial bribery, as well as for the promise or offer of mediation in commercial bribery;
- responsibility for commercial bribery is differentiated depending on the size of the subject of bribery;
- range of persons in relation to whom provocation of commercial bribery or bribery is possible is clarified;
- alternative types of punishment are envisaged for commercial bribery and bribery (in the form of a fine in absolute terms with the appointment of additional punishment in the form of deprivation of the right to hold certain positions/engage in certain activities for a long time).

The draft National Anti-Corruption Plan for 2018-2020 is at the final stage of agreement between state authorities.

Rosfinmonitoring together with representatives of the private sector is improving the model of financial behaviour of the "corrupt official" in order to subsequently introduce the appropriate profile in the internal control systems of financial organizations.

As a result of the measures taken (according to the Prosecutor General's Office of Russia) the number of revealed corruption violations has increased more than threefold since 2007, from 106,500 to 235,000 in 2016. More than 4,000 law enforcement officers and more than 400 regional and municipal deputies, almost 3,000 government officials and local self-government officials were convicted of corruption for the last 3,5 years. Corrupt persons for the last 2.5 years voluntarily repaid the damage to the state to the amount of about 10 billion rubles (more than 153 million USD).

INCREASED RISK GROUP

THE RISK OF ABUSING BANKS, MICRO-FINANCE COMPANIES AND CONSUMER CREDIT COOPERATIVES FOR ML PURPOSES

In order to suppress unlawful activities of managers and founders of financial institutions, the Criminal Code of the Russian Federation is supplemented with Article 17.1 ("falsification of financial documents of accounting and reporting by a financial organization") (*Federal Law No.218-FZ of July 21, 2014*).

The list of grounds for recalling a banking license from a credit institution has been expanded (*Federal Law No.484-FZ of December 29, 2014*).

The mandatory requirements to the qualifications and business reputation of members of management bodies, managers, responsible persons, owners (and their sole executive bodies) of credit institutions, insurance organizations, non-state pension funds, management companies of investment funds, mutual investment funds and non-state pension funds, microfinance companies are strengthened (*Federal Law No.281-FZ of July 29, 2017*). A cross-sectoral approach has been introduced to assess compliance with the requirements for the business reputation of these individuals. The list of persons to whom requirements for the business reputation are applied is supplemented by a person responsible for the implementation of the AML/CFT measures in these financial institutions. In a number of cases, a life-long ban on: participation in the management of a credit institution, the acquisition of a block of shares (stakes) in a credit institution, the establishment of control over owners of large block of shares (stakes) of a credit institution, taking the position of the sole executive body of a major shareholder (stakes) of credit institution (the controller of the owner) is established.

Rosfinmonitoring regularly communicates information to the Bank of Russia on the risks of abusing financial institutions for the purpose of conducting suspicious transactions.

With respect to micro-finance companies and consumer credit cooperatives, the Bank of Russia conducts supervisory activities and takes supervisory response measures the effectiveness of which is confirmed by a substantial reduction in the number of suspicious transactions in the microfinance sector. Such work is carried out, including, with respect to micro-finance companies and consumer credit cooperatives noted in the information provided by Rosfinmonitoring.

THE RISK OF ABUSING THE PRECIOUS METALS AND PRECIOUS STONES MARKET FOR ML PURPOSES

The program for establishing an integrated information panel in the sphere of control over the turnover of precious metals and stones at all stages has been approved.

Work is underway to improve the procedure for special registration regime of the industry representatives and to expand the powers of the supervisory authority, as well as to strengthen the sanctioning measures for violation of legal requirements.

New forms of information interaction and contactless control (such as Personal online account) between Rosfinmonitoring and Assay Chamber of Russia are actively developing.

THE RISK OF ABUSING MONEY TRANSFER SYSTEMS FOR ML PURPOSES

Rosfinmonitoring, together with experts from private sector organizations is updating the profile of a drug trafficker/drug dealer including those using money transfer systems. In the future, it is planned to introduce the updated profile into the internal control systems of financial organizations.

The materials of one financial investigation initiated as a result of such a public-private partnership contributed to the initiation of 10 criminal cases involving the seizure of about 30 kg of heroin and the arrest of 10 individuals on the territory of the Moscow region. It also helped to document the involvement in drug trafficking of more than 25 individuals as well as their financial connection with the OCGs and to seize approximately 100 kg of heroin.

THE RISK OF ABUSING THE SECURITIES MARKET FOR ML PURPOSES

Over the recent years a number of dishonest participants that did not comply with the requirements of the existing legislation, including the AML/CFT Law have been withdrawn from the market with their licenses being revoked.

The Bank of Russia, in order to reduce the risk of ML/FT for supervised subjects regularly issues sector-specific methodological recommendations on increasing attention to certain types of transactions, including on ML risks in the securities sector.

THE RISK OF CROSS-BORDER MOVEMENTS OF CURRENCY AND BEARER NEGOTIABLE INSTRUMENTS (BNIs) IN ML SCHEMES

Consideration is being given to making amendments to the EEU Agreement to secure the economic safety of participants not only in the sphere of customs regulation, but also from the AML/CFT perspective. This measure will provide legal conditions for the functioning of certain elements of the AML/CFT system in the EEU area.

The supra-national ML risk assessment within the framework of the Council of Heads of Financial Intelligence Units of the Member States of the Commonwealth of Independent States was recently initiated. One of the main areas of risk assessment: couriers cash.

MODERATE RISK GROUP

THE RISK OF ABUSING THE INSURANCE SECTOR IN SCHEMES OF LEGALIZATION OF CRIMINAL PROCEEDS

A number of insurance entities that did not comply with the requirements of the existing legislation, including the AML/CFT Law have been withdrawn from the market during the last couple of years with their licenses being revoked.

The Bank of Russia, in order to reduce the risk of ML/FT for supervised subjects regularly issues sector-specific methodological recommendations on increasing attention to certain types of transactions, including on ML risks in the insurance sector.

THE RISK OF USING REAL ESTATE IN SCHEMES OF LEGALIZATION OF CRIMINAL INCOMES

Measures taken by the government (constant updating of the cadastral value of real estate objects as a tax base, an increase in the period from 3 to 5 years during which the owner cannot sell the acquired real estate without paying income tax, an increase in the number of non-cash settlements, etc.) allowed to a certain extent reducing the risks of using real estate for ML purposes.

Work is underway to make sure that all real estate agents are engaged in the AML/CFT system, primarily through the mechanisms of the Personal online account on the official website of Rosfinmonitoring.

The role of preventive and corrective measures in reducing the risks in the real estate agents sector has significantly increased.

THE RISK OF ABUSING POSTAL REMITTANCES SERVICES FOR ML PURPOSES

A set of inter-ministerial measures were taken to mitigate the risks of abusing the services of the Russian Post for unlawful purposes.

In accordance with the Order of Rosfinmonitoring No.103, the mechanism of refusal to conclude contracts between the Russian Post and legal persons is applied and further monitoring of contracts is carried out in accordance with the criteria of this Order.

The sector is being informed about the ML/FT risks and the importance of proper implementation of the AML legislation provisions regarding the organization and implementation of internal controls.

THE RISK OF ABUSING NOTARIES FOR ML PURPOSES

Relevant information and methodological assistance on AML/CFT issues is being provided to notaries, including information on risks and typologies of possible abuse of notary deposit accounts and executive signatures for illegal purposes.

Rosfinmonitoring and the Federal Chamber of Notaries cooperate to ensure the participation of notaries in the AML/CFT system and to improve legislation. Lists of notaries whose activities may bear potential ML risks are sent to the Federal Notary Chamber for the subsequent application of supervisory measures.

The control over notaries acting in regions of the Russian Federation is strengthened.

The Code of Professional Ethics of Notaries in the Russian Federation was adopted (*approved by the Ministry of Justice of Russia on 19.01.2016*).

THE RISK OF ABUSING THE LEASING SECTOR FOR ML PURPOSES

In order to strengthen the legal framework in the leasing sector and further improve the state control and supervision over the sector, a draft federal law "On Amendments// to Certain Legislative Acts of the Russian Federation" has been drafted. The draft law provides for the introduction of a permitting system for admission of leasing companies to the market and a system of control (supervision) over the activities of entities (including their financial condition) by the Bank of Russia.

THE RISK OF ABUSING MOBILE PHONE OPERATORS FOR ML PURPOSES

In order to minimize the risks of abusing mobile phone operators for unlawful purposes, in particular for suspicious cash transactions, interagency cooperation is being carried out. Sector-specific recommendations on reducing the risks of possible involvement of mobile phone operators in ML processes are being prepared.

THE RISK OF ABUSING PAYMENT OPERATORS FOR ML PURPOSES

The Bank of Russia had taken measures to counter the practice of conducting high-risk transactions involving sale of cash delivered by natural persons to payment terminals. As a result, the cases of violation of the Federal Laws No. 103-FZ and No. 161-FZ in the sector were almost completely discontinued.

LOW RISK GROUP

THE RISK OF ABUSING OTHER FINANCIAL SECTORS AND DNFBPs (MUTUAL INSURANCE COMPANIES, MUTUAL INVESTMENT FUNDS, INVESTMENT FUND MANAGEMENT COMPANIES, PRIVATE PENSION FUNDS, AUDITORS, LAWYERS, FACTORING, GAMBLING SECTOR, ADVOCATES, ACCOUNTANTS) FOR ML PURPOSES

Coordinated inter-ministerial work is being carried out to increase the level of coverage of lawyers and auditors by the AML/CFT system.

Information and methodological support to advocates on AML/CFT issues, including risks and typologies was provided. Regular interaction with the regional lawyers' chambers is organized. Further steps will be taken to promote regular information exchange between the Federal Chamber of Advocates and Rosfinmonitoring.

The requirements for auditors in relation to AML/CFT issues have been clarified and specified *(the AML/CFT Law and Article 13 of Federal Law No. 307-FZ of 30 December 2008 "On Auditing" (in the wording of the Federal Law of April 23, 2018 No. 112-FZ). Individual auditors and audit organizations are required to notify the authorized body (Rosfinmonitoring) of any grounds to suspect that financial transactions or financial settlements of the audited entity are related to ML or TF. The auditors have no right to disclose the fact that this information is being filed, as well as to inform the management of the audited entity about the occurrence of the said suspicions. The order of information disclosure is determined by the Government of the Russian Federation. On the website of Rosfinmonitoring there are personal online accounts for user interaction with the FIU. In established cases, the accounts can be used by auditors).*

The involvement of gambling sector entities in the AML/CFT system has been increased and control measures have been improved.

Further steps will be taken to strengthen administrative liability for illegal organization and holding of lotteries and gambling (*draft Federal Law No. 1093505-6*).

Work is being carried out to increase the degree of use by the payment operators of the Personal Online Account on the website of Rosfinmonitoring in particular by promoting the advantages of using personal online accounts for the AML/CFT compliance purposes.

CONCLUSION

The work done on the national ML risk assessment allowed to identify the key risks, threats and vulnerabilities for the AML system in the Russian Federation at the moment.

Based on the results of this work an interagency Action Plan has been prepared to mitigate the identified risks and threats and to improve the effectiveness of the national AML system.

This Action Plan contains a list of preventive, regulatory, law enforcement and organizational measures, as well as measures aimed at improving the effectiveness of interagency and international cooperation and interaction with the private sector.

The law enforcement, control and supervisory authorities and other state bodies - stakeholders of the AML/CFT system are recommended to prioritize their further work taking into account the Action Plan measures in order to counteract major ML risks and threats, increase the security of the national financial system and improve the effectiveness of the Russian "anti-laundering" system.

Financial institutions and DNFBPs - subjects of the AML/CFT Law are recommended to use the results of ML NRA in their day-to-day work, when developing and applying a risk-based approach in their activities.

Moscow
2018