FINANCIAL SECURITY

NO. 27 JULY 2020

PANDEMIC AND RELATED ML RISKS

CONTENTS

EDITORIAL BOARD

Members of Editorial Board

DEAR READERS,

Greeting you from the pages of our journal, I experience mixed feelings. On the one hand, amid the coronavirus pandemic, the global AML/CFT framework faces completely new challenges and threats. On the other, our concerted efforts have enabled us to quickly adapt to new circumstances and respond to emerging risks.

COVID-19 has made changes not only to the international agenda (joint FATF/EAG Plenary meeting, scheduled to be held in China, and CIS Council of Heads of FIUs meeting were both held via video conferencing), but also to everyday life: unfortunately, some of our colleagues and loved ones have succumbed to the virus.

We have decided to dedicate this issue of "Financial Security" to the coronavirus problem, as viewed from the standpoint of the AML/CFT/PF system's response to possible financial consequences for the global economy and individual countries.

In these challenging times, close cooperation with the private sector remains highly relevant. The search for new modalities and approaches to supervision in the context of existing restrictive measures is of particular importance.

I wish you all good health and robust immune system!

Yury Chikhanchin,
Director of Rosfinmonitoring

COVER STORY: COVID-19 AND MEASURES TO COMBAT ILLICIT TRANSACTIONS

V. PUTIN: "I KNOW THAT THE SYSTEM WORKS"

A meeting of the President of the Russian Federation Vladimir Putin with the Director of Rosfinmonitoring Yury Chikhanchin took place in the Kremlin on 18 June 2020

The focus of the meeting was on the public funds monitoring results allocated for national projects.

According to the Director of Rosfinmonitoring, the supervision system has been put in place with the help of all stakeholders, with the Treasury of Russia, Federal Tax Service, General Prosecutor's Office and the Federal Security Service of Russia playing a major role.

"We've developed a cooperation mechanism and put in place an oversight system, which includes common approaches to risk assessment as well as risk monitoring system and mitigation mechanisms, with all new proposals being forwarded to the Russian Government."

Naturally, all these approaches proved to be useful in overseeing the public funds expenditure allocated to fight the coronavirus.

Rosfinmonitoring monitors about 7,000 COVID-19-related public contracts totalling RUR 11 billion awarded to 4500 different companies and individual entrepreneurs. To mitigate the risk of non-execution of these contracts, Rosfinmonitoring has assessed all contractors involved to identify those at higher risk, passing on some of its findings to law enforcement.

"To date, some of these contracts have been terminated and criminal investigations have been launched. This has allowed us to improve the situation, including compliance of the contractors involved in the COVID-19 response efforts. If you look at the graphs, you'll see declining trends across the board, including suspicious transactions and the use of shell companies...A similar situation exists in the procurement of medical equipment and artificial lung ventilation devices" explained Yury Chikhanchin.

The pandemic has also threatened systemic enterprises, which also found themselves in need of government support.

Background

Systemic enterprises are companies that, due to their status as some of the largest employers and taxpayers in their respective industries, play a major role in the country's economy.

The Russian government has launched a number of initiatives in support of systemic enterprises:

Subsidized loans to replenish working capital and maintain employment.

A 6-month bankruptcy moratorium.

Special conditions to apply for tax payment delay or to use instalment plans for tax payments due in 2020 – except for MET, excise taxes and petroleum profits tax – for companies whose revenues have declined by 10 percent or more.

Systemic enterprises facing higher risks may also apply for subsidies to cover the cost of manufacturing, execution of works and provision of services, as well as state guarantees needed to restructure existing debt and secure new loans, including bond loans.

The number of eligible enterprises currently stands at 1335.

Agencies involved in public procurement oversight

Law enforcement

FSB

Ministry of Internal Affairs

Investigative Committee

Supervisors

Rosfinmonitoring

FTS

General Prosecutor's Office

FAS

Federal Treasury

According to the Director of Rosfinmonitoring, among them there are companies previously identified by Rosfinmonitoring to be in «risk zone» for the falsification of financial statements and transfer of funds to entities registered abroad, including jurisdictions with preferential tax regimes. In addition, some of them are believed to have participated in transferring money to shadow turnover zone using «technical» companies, placement of funds in deposit accounts and appointment of foreign nationals to management positions in the company. All generated intelligence has been passed on to the Russian government for elaboration of new approaches.

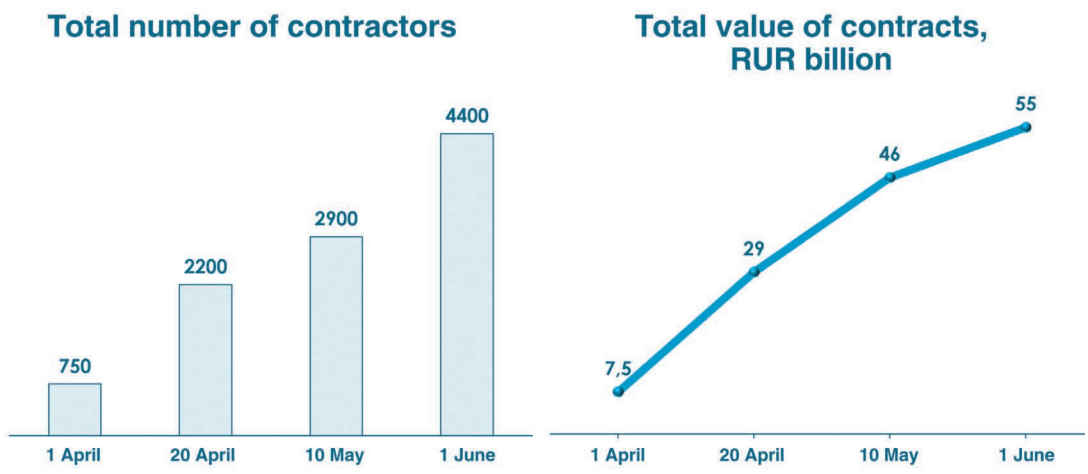
While reporting to the President of the Russian Federation on the overall situation with national projects, Chikhanchin pointed out that about one-third of contractors are currently believed to be at risk, with some, according to intelligence provided by financial institutions, being linked to a significant number of suspicious transactions or displaying signs of fictitiousness.

V. Putin: *"Although they may not necessarily be shell companies, they weren't set up for legitimate business either."*

Yu. Chikhanchin: That's right. Despite their recent incorporation, they're already targeting contracts worth billions. And we, in collaboration with other agencies, are monitoring their activities...If we look at the districts where national projects are being implemented, the Southern Federal District and the Far Eastern Federal District are of the biggest concern. We're working closely with the offices of plenipotentiary representatives in these districts to keep them updated in advance on the risks we see and developing ways to mitigate them. As for the constituent entities, some of them do face risks, i.e. the Stavropol Territory, the Penza Region and the Khabarovsk Territory."

In addition, the Director of Rosfinmonitoring reported to the President of the Russian Federation on the agency's cooperation with governors, particularly in implementing pilot projects in the Novgorod and

Awarded contracts in the framework of countering COVID-19 pandemic



Out of a total of **7000 contracts, more than 2700** were awarded to **1300** companies for the supply of artificial lung ventilation devices and other related equipment totalling **RUR 42 billion**

Tula Regions. Rosfinmonitoring engages closely with the governments of these regions to take preventive actions against the identified risks. To this end, the competent authorities, working in collaboration with the contracting authorities, used Rosfinmonitoring's intelligence to monitor the execution of public contracts awarded to certain contractors and to assess the level of risk each of them face. Following a review of the outcomes of this engagement, the Russian government recommended it for adoption across the country.

Rosfinmonitoring, in cooperation with the Federal Antimonopoly Service and FSB, uncovered violations of the antitrust laws totalling RUR 700 million in 2020 alone. The subsequent termination of the contracts and initiation of 50 criminal proceedings helped prevent the loss of RUR 3.8 billion in public funds, resulting in the recovery of damages totaling RUR 3 billion and seizure of another RUR 2 billion.

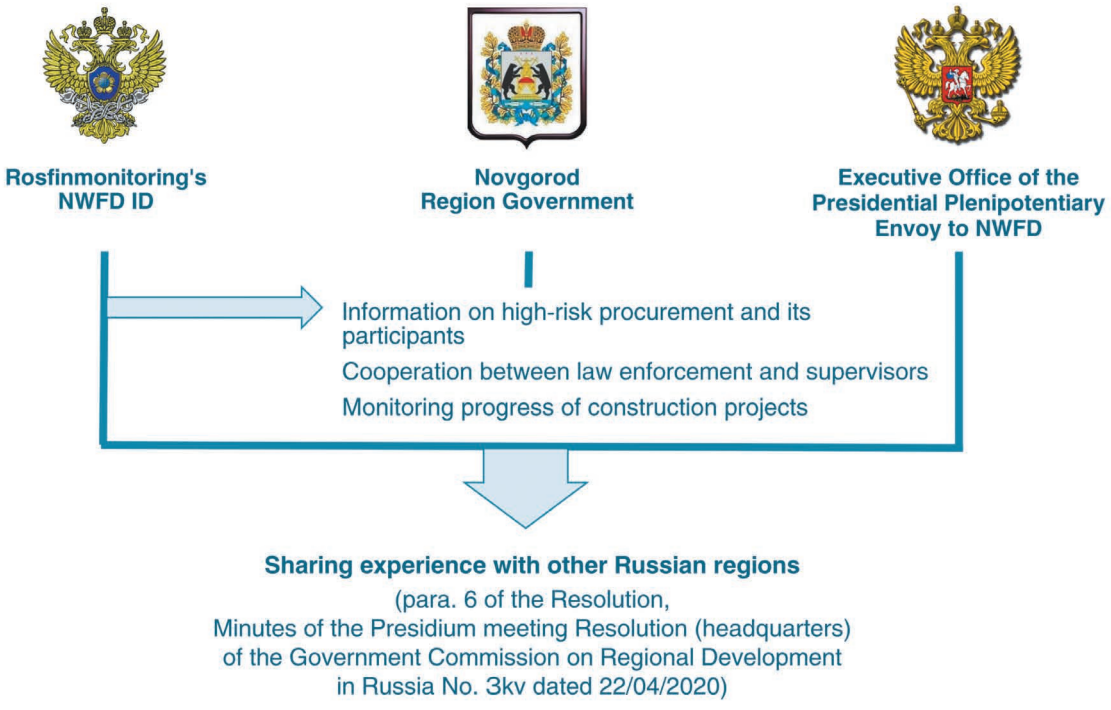
V. Putin: *"It's important to make sure that these cases reach court without getting side-tracked on their way there."*

Yu. Chikhanchin: *"We'll do our best."*

The Director of Rosfinmonitoring proposed the following approaches to improving public procurement oversight:

- to develop a mechanism for colour-coding public funds to enable their traceability all the way from contract authorities to individual contractors and sites;
- to adopt, at the interagency level, a unified risk classification system linked to non-implementation/improper implementation of national projects, and to promote the sharing of information on risks among the agencies concerned in accordance with the said classification system;
- to examine the possibility of establishing a Public Procurement Oversight Centre within the Russian government to coordinate supervisors' efforts and develop measures to improve efficiency in this area.

Pilot projects in Novgorod and Tula Regions



Almost all of the proposed approaches have already been implemented in the oversight of defence procurement.

Yu. Chikhanchin: *"I think it's important to acknowledge that the work done by us here back in 2016 has borne fruit, allowing us to reduce the number of dubious transactions by 35-37 percent and by as much as threefold in some areas, with almost no shell companies present and no bank refusals to carry out transactions issued to defence procurement contractors. In other words, we've managed to stabilize the situation and must now work on maintaining this stability."*

V. Putin: *"I know that the system recently put in place works."*

Yu. Chikhanchin: *"Indeed."*

According to the Director of Rosfinmonitoring, the decision to designate Promsvyazbank, which currently handles 58 percent of defence procurement contracts, as the chief financial institution for defence procurement funds contributed to the implementation of the plan.

Yu. Chikhanchin: *"Thanks to the work carried out jointly with the Central Bank and law enforcement – primarily FSB, the Ministry of Internal Affairs and the General Prosecutor's Office – we've succeeded in cleaning up the banking sector, getting rid of unreliable banks. And while only 18 months ago we talked about several dozen ML centres operating in the country, today there're only about a dozen of them left in total. We're aware of their existence and beginning to take steps to dismantle them.*

COVID-19 PANDEMIC RELATED ML/TF RISKS AND RESPONSE MEASURES: RUSSIAN AND INTERNATIONAL EXPERIENCE

Evgeny Mozgov,
Head of Rosfinmonitoring's Risk Assessment Department

Olga Pershina,
Consultant at Rosfinmonitoring's Risk Assessment Department

The COVID-19 pandemic has presented new challenges and threats to the Global AML/CFT Network.

As an integral part of the state machinery, the Russian AML/CFT framework contributes to the efforts to identify and mitigate the ML/TF risks stemming from COVID-19 pandemic. The Russian Federal Financial Monitoring Service sees its priorities today in assessing the impact of the current crisis on the ML/TF risks and formulating response measures.

The emerging pattern of ML/TF risks allows us to conclude that the pandemic has increased the risks linked to certain predicate offences.

One of the most widespread trespassing is fraud. Criminals seek to take advantage of the current crisis to make illegal online sales of personal protective equipment, COVID-19 tests and medicines, without actually shipping them to the customer. Against the backdrop of widespread flight cancellations caused by the pandemic, fraudsters' arsenal of illicit schemes has been expanded to include scams involving ticket refunds. Meanwhile, the government's stimulus measures have been linked to fraudulent schemes involving relief assistance allocated for certain categories of the population. The pandemic has also been accompanied by emergence of illicit schemes linked to employment, tax payments and investments.

Financial institutions have recorded a sharp increase in cyber fraud cases involving methods of social engineering and phishing attacks. It is quite common for criminals to send out phishing emails containing links to fake or virus-infected sites in order to steal bank card details and withdraw funds, including those appearing to be from the World Health Organization as well as from charity campaigns sponsored by the World Bank and IMF.

The unprecedented measures being taken by the Russian government to stabilize the economy, coupled with the loosening of procurement requirements, have increased the risk of COVID-19 relief funds embezzlement.

Particularly risky in this context are the fundraising campaigns run by non-profit organizations presumably for public relief, with proceeds going into the shadow economy. As a result, all fundraising initiatives attempting to raise money online are subject to extra scrutiny.

Rosfinmonitoring carries out regular assessments of the potential ML/TF risks related to the pandemic and communicates findings to law enforcement.

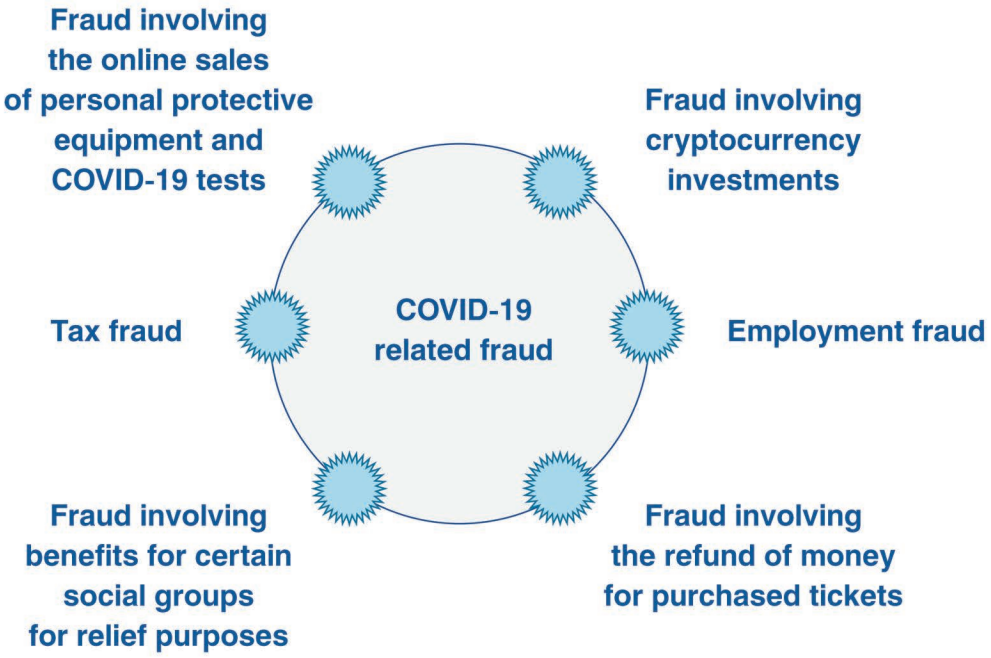
As part of the efforts to mitigate the risks of illegal fund transfers being disguised as payments for various medical products and medical equipment, Rosfinmonitoring analyses the relevant suspicious transactions and shares with law enforcement the intelligence on possible pass-through and cash-out transactions carried out by unscrupulous entities under the guise of legitimate trade in medical and personal protective equipment.

A key focus area in Rosfinmonitoring's efforts is the scrutiny of public anti-COVID-19 tests contracts to identify suspicious transactions involving possible misuse of public funds as well as unreliable contractors.

In addition, due to the risks linked to fundraising campaigns run by fake charities, extra efforts need to be dedicated to the analysis of open source data on charitable donations in order to identify persons raising funds for criminal purposes.

As part of its engagement with the private sector, Rosfinmonitoring shares with reporting entities information on the said risks and proposed identification measures, by posting it on its official website as well as in the Personal accounts of reporting entities. One such information statement points out that, against the backdrop of the COVID-19 pandemic, preventive measures, undertaken without delay by financial and other institutions as part of compliance procedures, must remain among top priorities in the efforts to prevent the intensification of illicit activities as well as terrorism and extremism. Given the need to prioritize these procedures and apply a risk-based approach to the allocation of resources in the current situation, the relevant information and guidelines on reporting suspicious transactions in the presence of the aforementioned risks are posted to the Personal accounts of reporting entities.

Common types of fraud



Potential ML/TF risks

To reduce the regulatory pressure on the private sector in the period of the pandemic, Rosfinmonitoring has cancelled all AML/CFT compliance audits planned for this year, except for special circumstances, which should reduce the overall administrative burden on businesses without exempting them from the responsibility to comply with AML/CFT requirements.

At the same time, Rosfinmonitoring continues to monitor compliance of reporting entities with AML/CFT requirements remotely.

At the supranational level, organizations working to maintain the stability of the global financial system have been tasked with assessing the impact of the pandemic on ML/TF risks and identifying best practices and responses to emerging threats and vulnerabilities. In particular, the FATF has reviewed its members' experience in identifying potential ML/TF risks and responding to them. Rosfinmonitoring, for its part, has promptly informed the FATF about our country's AML/CFT efforts to counter COVID-19 pandemic challenges.

After completing its review, the FATF published a report on the common threats, vulnerabilities and risks currently faced by national AML/CFT systems.

Potential COVID-19 pandemic related ML/TF risks identified in the report are:

- Increased misuse of online financial services and (or) virtual assets for ML purposes;
- Exploiting temporary challenges in exercising internal controls caused by remote working situations, in order to bypass CDD measures;
- A potential increase in the number of transactions that are not consistent with the customer profile, increased use of the unregulated financial sector, and massive cash flows;
- Misuse of legal entities to get access to stimulus payments for further laundering, misuse of legitimate enterprises or concealment of assets by initiating insolvency procedure.
- Criminals and terrorists moving into new cash-intensive and high-liquidity lines of business, including for ML purposes.

Among the priority response measures undertaken by all countries identified in the report are: strengthening communication with the private sector, encouraging the full use of a risk-based approach to customer due diligence, supporting electronic and digital payment options, undertaking pragmatic, risk-based AML/CFT supervision, clarifying AML/CFT requirements in the context of economic relief measures, continuing cooperation across borders, and monitoring the impact of COVID-19 pandemic on the private sector.

The work to gather up-to-date information on the main predicate offences, threats, vulnerabilities as well as on the best law enforcement practices and experiences is also carried out by the MONEYVAL and the EAG.

Notably, measures being undertaken by countries to mitigate the ML/TF risks linked to the pandemic were frequently discussed at FATF, MONEYVAL and EAG online meetings, generating considerable interest in the audience. In this regard, representatives of the Russian Federation attending working meetings keep their colleagues up to date with Russia's experience in combating financial crimes during the pandemic situation.

Analysis of open source data, including the official websites of foreign financial intelligence units (FIUs), shows that AML/CFT foreign officials fighting the COVID-19 pandemic face similar ML/TF risks. In this regard, it might be useful to examine how the COVID-19 pandemic is affecting the ML/TF risks and responses in some countries.

In the midst of the pandemic in the United States, the Financial Crimes Enforcement Network (FinCEN), the US FIU, released a statement urging financial institutions to inform FinCEN and their functional regulators about potential issues related to any potential delays in their ability to file required Bank Secrecy Act (BSA) reports during the COVID-19 pandemic. At the same time, the US FIU notes the following COVID-19 related emerging trends:

- Fraud Scams – Bad actors attempt to solicit donations, steal personal information, or distribute malware by impersonating government agencies, international organizations, or healthcare organizations;
- Investment Scams – The U.S. Securities and Exchange Commission (SEC) cautioned investors against COVID-19-related investment scams, such as promotions that falsely claim that the products or services of publicly traded companies can prevent, detect, or cure coronavirus;
- Product Scams – The U.S. Federal Trade Commission (FTC) and U.S. Food and Drug Administration (FDA) have issued public statements and warning letters to companies selling unapproved or misbranded products that are particularly in demand during the pandemic;
- Insider Trading;
- The US FIU particularly urges financial institutions to implement a risk-based approach and ensure good faith compliance with the Bank Secrecy Act. It is also worth noting that the US FIU has created a special online mechanism through which financial institutions can inform, on a voluntary basis, the FIU about the risks of non-compliance with AML/CFT requirements.

The US FIU uses newsletters published on its website to inform reporting entities and other interested parties about various types of consumer fraud, as well as to update them on the prevalent types of fraud in the medical field. These updates include descriptions of various scams as well as indicators designed to enable timely detection and prevention of criminal activity against the background of COVID-19.

The official website of the Financial Transactions and Reports Analysis Centre of Canada, Canada's financial intelligence unit, also contains recommendations for reporting entities on compliance with AML/CFT requirements. In particular, it states that reporting entities should give priority to submitting suspicious transaction reports. In exceptional circumstances when a reporting entity may be in possession of critical information related to terrorist financing but, for some reason, cannot submit the STR in the usual manner, FINTRAC asks to send STRs to the email address specified on its website.

In other instances where a reporting entity cannot file STR or reports suspicious transactions with delay for reasons beyond its control, the entity can submit a voluntary self-declaration of non-compliance with STR submission requirements.

ML/TF risks similar to those faced by Russian authorities have been identified by the UK National Crime Agency. The agency's website contains guidelines for dealing with various types of fraud prevalent during the COVID-19 pandemic, including those associated with online shopping, holding auctions, installing malicious software, and attracting investment.

To improve the processing of incoming STRs, the UK has introduced special codes which are used by entities wishing to report any attempts made by criminals to use the COVID-19 pandemic for their advantage.

Much has been done by Europol to describe the current pattern of risks and offences identified against the backdrop of the COVID-19 pandemic. Of particular interest is Europol's publications on the impact of the COVID-19 pandemic on EU drug markets. According to the paper, the travel restrictions introduced by various countries around the world have temporarily disrupted the drug market, resulting in shortages of certain banned substances and, as a result, higher prices. According to the report, disruption to the drug trafficking supply chain is seen mostly at the distribution level, due to social distancing measures within the EU.

But while the logistics may have changed, the movement of bulk quantities of drugs between EU member states has not ceased, despite border controls, due to the continued commercial transportation of goods across Europe. Organised crime groups are adapting their modi operandi to the current situation, further exploiting secure communication channels and adapting transportation models, trafficking routes and concealment methods.

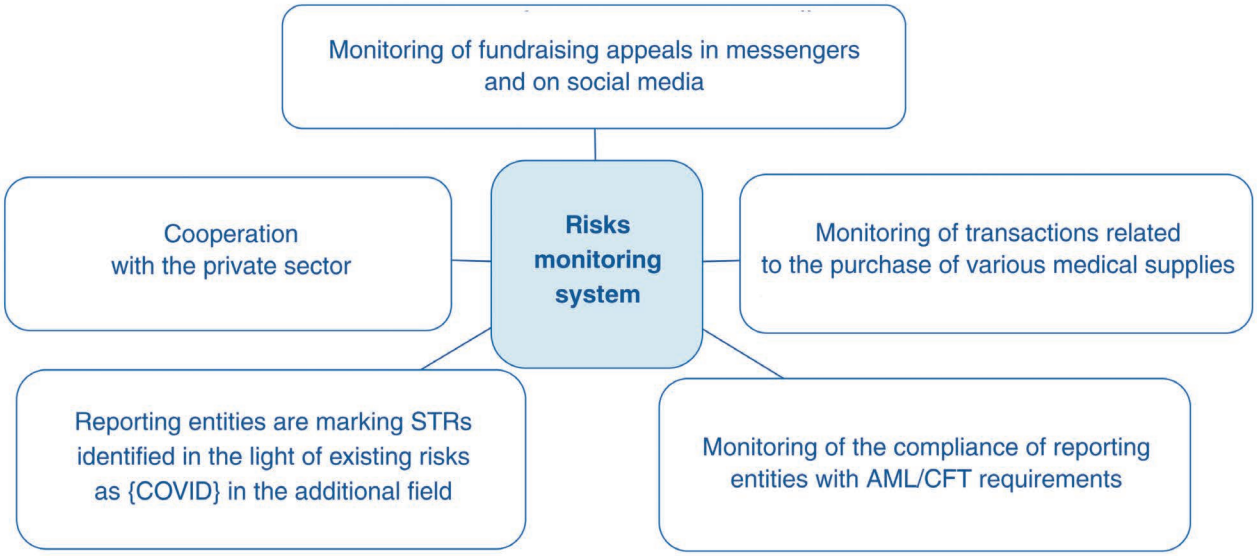
The report notes that surface web and darknet markets, social media and internet secure encrypted communication applications now appear to be playing a more prominent role in the drugs distribution at user level.

In addition, according to the information released by Europol, the COVID-19 crisis has led to a sharp increase in the distribution of content related to the sexual exploitation of children. Due to the social distancing measures adopted across the EU, criminals are shifting their focus to the online sharing of illicit content.

In one of its recently published studies on cyber-fraud, Europol notes a spike in this type of crimes recorded during the COVID-19 pandemic. Cyber criminals have rapidly adapted to the new status quo to take advantage of economic instability, fear and confusion felt by the public. At the same time, the agency expects the scale of phishing and extortion attacks carried out by cyber fraudsters to increase further.

In addition, analysis of the organized criminal groups' activities ("OCGs") carried out by Europol shows that large OCG might exploit the current crisis for ML purposes by involving in this process countries with a weak AML/CFT regulatory framework and low barriers to the import of large volumes of capital from dubious sources.

Adopted ML/TF mitigation measures



In view of the foregoing, it can be concluded that the COVID-19 pandemic has affected various components of the AML/CFT regime. National AML/CFT systems around the world are faced with new challenges, threats and previously unidentified risks.

In this regard, we must acknowledge the relevance of the work currently being carried out by Rosfinmonitoring in collaboration with the FIUs of the CHFIU member-states to establish an International ML/TF Risk Assessment Centre (IRAC).

The establishment of the IRAC, an international service platform, will facilitate the sharing of strategic and tactical intelligence and information about the identified ML/TF risks. In addition, the IRAC will help national AML/CFT systems to better prepare for new challenges and threats, and most importantly, promptly identify potential ML/TF risks and take steps, both within the framework of IRAC participants' national AML/CFT system and at the supranational level, to mitigate them.

RISKS LINKED TO THE EMBEZZLEMENT OF PUBLIC FUNDS, PRIVATE AND CORPORATE PROPERTY DURING THE CORONAVIRUS PANDEMIC SITUATION

Olga Tisen,
Head of Rosfinmonitoring's Legal Department, PhD

The Federal Financial Monitoring Service has conducted an assessment of threats to national security linked to transactions with funds or other assets in the coronavirus pandemic situation. The economic crisis provoked by COVID-19 will result in increase in the number of offences involving the embezzlement of public funds, including those allocated to combat the pandemic and its consequences. Furthermore, it has led to the emergence of new types of fraud fuelled by the increased demand for personal protective equipment and medicines, as well as by public fear of getting infected, losing jobs and sources of income.

As it stands, crimes involving the embezzlement of public funds and corruption tend to remain undetected long after they have been committed. Hence, we need to take urgent measures to ensure their timely identification and suppression. To facilitate the timely identification and suppression of crimes linked to the embezzlement of public funds and other property offences, Rosfinmonitoring has identified the key patterns of criminal conduct particularly prevalent during the pandemic. When studying the key COVID-19 related embezzlement risks, Rosfinmonitoring considered, among others, the experience of other countries and information on emerging ML/TF risks prepared by the FATF Secretariat.

Risks of embezzlement of COVID-19 relief funds

1. Public procurement risks

To streamline the public procurement procedures in the period of the coronavirus pandemic, Federal Law No. 98-FZ of April 1, 2020 "On Amendments to Certain Legislative Acts of the Russian Federation Concerning the Prevention and Management of Emergency Situations" amended Federal Law No. 44-FZ of April 5, 2013 "On the Contract System in State and Municipal Procurement of Goods, Works and Services," enabling the purchase of any goods, works or services from a single contractor, irrespective of their inclusion in the list, authorized by the Russian government, as well as other measures[1].

Until December 31, 2020, customers participating in the procurement process are not required to include in the tender notification and (or) draft contract the demand for execution of the contract or fulfillment of warranty obligations, unless the contract provides for advance payment.

In addition, in 2020, subject to the occurrence of circumstances beyond the control of the parties brought about by the spread of the coronavirus infection or in other cases envisaged by the Russian government that render the implementation of the contract impossible, the parties to the contract, by mutual agreement, may change the contract term[2] or its price.[3]

On 24 April 2020, Federal Law No. 44-FZ "On the Contract System in State and Municipal Procurement of Goods, Works and Services" was again amended to streamline the public procurement procedure, i.e. the maximum value of a contract entered into with a single supplier was increased twofold: from RUR 300,000 to 600,000, and the minimum amount of contract execution guarantee was reduced from 5 to 0.5 percent of the initial price.[4]

It means that COVID-19 relief funds can currently be spent without due competitive procedures, with purchases often made from a single supplier. All this creates the risk of goods being bought at inflated prices or the pandemic being used to purchase goods and services not related to the efforts to combat it. There is also a high likelihood of public funds being fictitiously used for certain purposes while actually being embezzled and contractors citing the pandemic as an excuse for non-execution of public contracts.

Possible abuses of public procurement procedures to embezzle COVID-19 relief funds:

1. Purchase of goods, medical equipment, products, consumables and personal protective equipment at inflated prices

The easing of restrictions related to the procurement of goods from a single supplier increases the risk of purchases being made at inflated prices. The likelihood of such abuses is particularly high in situations involving the purchase of medical devices, goods and personal protective equipment, whose use in public places became mandatory in many Russian regions, including Moscow, starting 12 May 2020.

The enactment of Presidential Decree No. 316 dated 11 May 2020[5], which lifted restrictions on the manufacturing, construction and other sectors, inevitably created high demand for masks, gloves and non-contact thermometers, thereby increasing the risk of their purchase at inflated prices.

Thus, the public procurement website, which is accessible to the public, contains information about the purchases of medical supplies made as of 12 May 2020 using a simplified procedure due to the coronavirus, with significant variations in prices.

---

[1] Federal Law No.98-FZ of April 1, 2020 "On Amendments to Certain Legislative Acts of the Russian Federation Concerning the Prevention and Management of Emergency Situations"

[2] Finance Ministry Letter No. 24-06-08/24649 dated March 27, 2020 "On Procurement Effected on Non-business Days"

[3] The Government of the Russian Federation Resolution No. 443 dated April 3, 2020 "On the Specifics of Procurement during the Period of Taking Measures to Ensure the Sanitary and Epidemiological Well-being of the Population in the Russian Federation in Connection with the Spread of the Novel Coronavirus Infection"

[4] Federal Law No. 124-FZ of 24 April 2020 "On Amendments to Certain Legislative Acts of the Russian Federation to Endure the Sustainable Development of the Economy in a Deteriorating Situation Caused by the Spread of the Novel Coronavirus Infection"

[5] Presidential Decree No. 316 dated 11 May 2020 "On the Procedure for Extending the Measures Needed to Ensure the Sanitary and Epidemiological Well-being of the Population"

For example, the price of non-contact infrared thermometers purchased for public needs during the pandemic fluctuates between RUR 7800 and 28,000, thermal cameras between RUR 740,000 and 1.2 million, and protective gowns of the same type and from the same manufacturer between RUR 554 and 3600 per item.

Significant differences in prices are also observed in the procurement of other medical goods made in response to the spread of the coronavirus infection, such as medical masks, equipment, etc. At present, the Federal Anti-Monopoly Service continues to identify cartel agreements in the markets for food products, medical equipment, goods and consumables, as well as instances of essential goods being sold at inflated prices during the pandemic.

These practices may point to the overstatement of the cost of identical goods and, accordingly, the price of government contracts, to enable the embezzlement of public funds, and must be investigated.

Officials found to be engaging in such practices may, depending on the circumstances of the offence, be charged with offences falling under Arts.159 "Fraud," 160 "Embezzlement or Misappropriation," 285 "Abuse of Office" 285.1 "Misappropriation of Public Funds," and 286 " Abuse of Public Authority" of the Criminal Code of the Russian Federation.

Meanwhile, unscrupulous suppliers may be charged with offences falling under Arts. 159 "Fraud" and 327 "Document Forgery" of the Criminal Code of the Russian Federation.

2. Misuse of simplified public procurement procedures to purchase goods not related to anti-COVID-19 efforts

The easing of public procurement restrictions may result in purchases of goods, works and services not related to the pandemic at inflated prices.

According to clarifications issued by the Ministry of Finance, the Anti-Monopoly Service and the Ministry of Emergency Situations[6], when making COVID-19 relief-related purchases, customers are required to ascertain the existence of a causal relationship between the procurement object and its intended use in meeting anti-COVID-19 needs and (or) preventing an emergency situation (introduction of a high alert state).

Notably, purchases from a single supplier may only be made in urgent situations for the purpose of prevention or elimination of the consequences of the spread of the coronavirus infection in accordance with Art. 93, pars. 4, 5 and 9 of part 1, of Law No. 44-FZ. This provision allows necessary purchases of medical masks, thermometers, disinfectants and other products needed during the pandemic.

First of all, simplified public procurement procedures can be used by entities that, pursuant to Presidential Decrees No. 239 dated 2 April 2020, No. 294 dated 28 April 2020 and No. 316 dated 11 May 2020, did not suspend their operations during the non-working period of between 1 April and 12 May 2020, as well as entities whose operations were not suspended by the regional governor[7].

If a person found engaging in such practices is an official, then depending on the circumstances of the offence, this person may be charged with offences falling under Arts.159 "Fraud," 160 "Embezzlement or Misappropriation," 285 "Abuse of Office" 285.1 "Misappropriation of Public Funds," 286 "Abuse of Public Authority" and 292 "Forgery by an Official" of the Criminal Code of the Russian Federation.

Meanwhile, unscrupulous suppliers may be charged with offences falling under Arts. 159 "Fraud" and 327 "Document Forgery" of the Criminal Code of the Russian Federation.

3. Use of the COVID-19 pandemic as an excuse for non-execution of public contracts

According to the joint letter of the Ministry of Finance, Ministry of Emergency Situations and FAS No. 24-06-05/26578/219-AG-70/ME/28039/20 dated 3 April 2020,

[6] Paragraphs 1 and 2 of Finance Ministry Letter No. 24-06-05/26578, Ministry of Emergency Situations Letter No. 219-AG-70 and FAS Letter No. ME/28039/20 dated 3 April 2020.

[7] RAS Letter No. ME/28054/20 dated 5 April 2020 "On Operations of Electronic Platform Operators in the Period until April 30, 2020"

the spread of the novel coronavirus infection caused by 2019-nCoV constitutes an emergency that cannot be avoided, hence its classification is force majeure. If any non-fulfillment or improper fulfillment of contractual obligations is caused by the coronavirus pandemic, the contractor (supplier) may cite this circumstance as a basis for exemption from payment of forfeit penalties (fines)[8].

Due to the pandemic, the Government of the Russian Federation Resolution No. 591[9] dated 26 April 2020 amended regulations governing the suspension of forfeit penalties previously adopted by the Government of the Russian Federation Resolution No. 783 dated 4 July 2018, which establishes the procedure for the writing off of forfeit penalties for non-fulfillment of contractual obligations in 2020 due to the pandemic. The adoption of relief measures for businesses allowing the writing off of accrued and unpaid forfeit penalties (fines) for non-fulfillment of prior commitments increases the risk of non-performance of public contracts under the pretext of difficulties caused by the pandemic.

When assessing compliance of contractors with applicable law, one must determine whether the contractor in question represents one of the sectors of the Russian economy most affected by the pandemic as per the list approved by the Government of the Russian Federation Resolution No. 434 dated 3 April 2020 (as amended 18 April 2020)[10].

Meanwhile, unscrupulous suppliers may be charged with offences falling under Art. 159 "Fraud" and 327 "Document Forgery" of the Criminal Code of the Russian Federation.

4. Disguising public funds as being spent for legitimate purposes while actually embezzling them

Given the disposable nature of many COVID-19 products (masks, gloves, protective suits, disinfectants, etc.), it may be difficult to verify the fact of their

actual purchase. Consequently, there are high-risk offences linked to embezzlement of public funds allocated for the purpose of meeting sanitary and epidemiological standards during the pandemic without actual supply of goods, performance of works and provision of services.

Officials found to be engaging in such practices may, depending on the circumstances of the offence, be charged with offences falling under Arts.159 "Fraud," 160 "Embezzlement or Misappropriation," 285 "Abuse of Office," 285.1 "Misappropriation of Public Funds," 286 " Abuse of Public Authority " and 292 "Forgery by an Official" of the Criminal Code of the Russian Federation.

Meanwhile, unscrupulous suppliers may be charged with offences falling under Arts. 159 "Fraud" and 327 "Forgery" of the Criminal Code of the Russian Federation.

5. Sale of low-quality, counterfeit or expired products unsuitable for intended use

According to clarifications given in pars. 2-5 of the Plenum of the Supreme Court of the Russian

[8] Joint letter of the Finance Ministry, Ministry of Emergency Situations and FAS No. 24-06-05/26578/219-AG-70/ME/28039/20 dated 3 April 2020

[9] The Government of the Russian Federation Resolution No. 591 dated 26 April 2020 "On Amending Government Resolution No. 783 dated 4 July 2018"

[10] The Government of the Russian Federation Resolution No. 434 dated 3 April 2020 (as amended 18 April 2020) "On approval of the list of sectors of the Russian economy most affected by the worsening COVID-19 situation"

Federation Resolution No. 48 dated 30 November 2017 "On judicial practice in proceedings related to fraud, misappropriation and embezzlement," such actions may be covered by Article 159 "Fraud" of the Criminal Code of the Russian Federation.

The embezzlement in this case is committed through deception: a deliberate communication (presentation) of deliberately false or inaccurate information, omission of facts, or deliberate actions (e.g. the provision of fake goods or other contractual items) aimed at misleading the owner of the property or another person[11].

Actions by unscrupulous suppliers may constitute offences covered by Arts.159 "Fraud" and 327 "Forgery" of the Criminal Code of the Russian Federation.

All above offences may be predicate to money laundering.

Risks linked to the embezzlement of COVID-19 relief funds intended for businesses and individuals

Faced with the coronavirus pandemic, the Russian government has taken measures to support the country's economy[12]. Thus, to support manufacturers and other businesses included in the list of sectors of the Russian economy most affected by the worsening COVID-19 situation[13], the Government of the Russian Federation has adopted the following economic measures:

- postponement of payment of tax and insurance premium payments reduction of payments[14];
- direct budgetary allocations[15];
- subsidies, soft loans and credit holidays[16];
- a bankruptcy moratorium[17];
- reduced supervisory burden[18];
- relaxation of licensing and other authorization procedures;
- rent payment holidays;
- free force majeure certificates;
- reduced acquiring commissions for online sale of goods;
- exemption from administrative fines for currency violations;
- postponement, by six months, of the entry into force of the requirement for mandatory pre-installation of Russian software;
- support for suppliers under government contracts;
- support for developers;
- suspension of fines for late payment of utility bills;
- support for tour operators.

[11] Paragraph 2 of the Plenum of the Supreme Court of the Russian Federation Resolution No. 48 dated 30 November 2017 "On judicial practice in proceedings involving fraud, misappropriation and embezzlement"

[12] The Government of the Russian Federation Decree No. 409 dated 2 April 2020 (as amended 24 April 2020) "On measures to promote the sustainable development of the economy" (together with the "Rules for granting deferrals (installment plan) for tax payments, advance tax payments and insurance premiums"

[13] The Government of the Russian Federation Resolution No. 434 dated 3 April 2020 (as amended 18 April 2020) "On approval of the list of sectors of the Russian economy most affected by the worsening COVID-19 situation"

[14] Federal Law No. 121-FZ of 22 April 2020 "On amendments to the Criminal Procedure Code of the Russian Federation"

[15] The Government of the Russian Federation Decree No. 576 dated 24 April 2020 "On approval of the Rules for the provision of federal subsidies to small- and medium-sized businesses operating in the sectors of the Russian economy in 2020 most affected by the worsening COVID-19 situation"

[16] Federal Law No. 106-FZ of 3 April 2020 "On amendments to Federal Law 'On the Central Bank of the Russian Federation (Bank of Russia)' and certain legislative acts of the Russian Federation concerning changes to the terms of loan agreements"; Bank of Russia Information Letter dated 17 April 2020 "The Bank of Russia has approved additional measures to protect the interests of citizens, ensure the flow of credit to the economy and temporarily loosen the requirements for compliance with AML/CFT and currency controls"

[17] The Government of the Russian Federation Resolution No. 428 dated 3 April 2020 "On the introduction of a moratorium on the initiation of bankruptcy proceedings at the request of creditors against individual debtors"

[18] The Government of the Russian Federation Decree No. 438 dated 3 April 2020 (as amended 22 April 2020) "On the specifics of state control (supervision), municipal control in 2020 and on amendments to paragraph 7 of the Rules for the preparation by state and municipals supervisors of annual plans for scheduled inspections of legal entities and individual entrepreneurs"

This increases the risk of relief funds embezzlement by entities not eligible to apply for them or claims for subsidies in excess of permitted amounts.

We are also very likely to see relief claims coming from businesses representing industries only mildly impacted by the spread of the novel coronavirus.

The Government of the Russian Federation Resolution № 576 dated 24 April 2020[19] provides for the provision in 2020 of federal relief funding to small and medium-sized businesses included, as of 1 March 2020, in the Unified Register of Small and Medium-Sized Businesses in accordance with the Federal Law "On the Development of Small and Medium-sized Businesses in the Russian Federation," which operate in the sectors of the Russian economy most affected by the spread of the coronavirus infection.

Notably, the purpose of these subsidies is to partially reimburse expenses of businesses incurred as a result of their continued operation during the pandemic, including for the retention of their staff and payment of wages, in April and May 2020.

These actions may result in the embezzlement of billions of rubles without any possibility of their recovery. In this regard, one of our top priorities for the immediate future should be the verification of businesses' eligibility to claim COVID-19 relief funding.

In addition, on 11 May 2020, the Russian President unveiled a new credit program in support of public employment. It provides for the issuance of loans in the amount of 1 minimum wage per employee per month for 6 months until 1 April 2021. If, during the term of the credit program, the business retains 90% of its employees or more, its loan and all interest accrued thereon will be written off after the expiration of the loan term.

However, this creates the risk of businesses misreporting their employment figures to gain access to relief funds and soft loans. Deliberately false information may also be provided by businesses in order to qualify for repayment holidays, tax breaks, bankruptcy moratoriums, etc.

Filing COVID-19 relief claims by ineligible businesses may constitute offences falling under Art. 199.2 of the Criminal Code "Concealment of the Entity or Individual Entrepreneur's Funds or Property Eligible to Be Used for Tax, Fee or Insurance Premium Collection Purposes."

The provision of deliberately false information in order to qualify for preferential loans may be covered by Art. 159.1 of the Criminal Code "Credit Fraud," i.e. the embezzlement of funds by the borrower achieved through the submission of deliberately false and (or) inaccurate information to the bank or other lender. According to clarifications given in para 7 of the Plenum of the Supreme Court Resolution No. 48 dated 30 November 2017 "On judicial practice in proceedings involving fraud, misappropriation and embezzlement," the use of forged documents granting relief from obligations may additionally be punishable under Art. 327 of the Criminal Code of the Russian Federation.

[19] The Government of the Russian Federation Decree No. 576 dated 24 April 2020 "On approval of the Rules for the provision of federal subsidies to small- and medium-sized businesses operating in the sectors of the Russian economy in 2020 most affected by the worsening COVID-19 situation"

The provision of deliberately false information as a way to gain eligibility for COVID-19 relief funding is punishable under Art. 159.2 of the Criminal Code "Access to Payments Fraud."

It should be borne in mind that investigations into these criminal activities may uncover evidence of offences falling under Art.199.4 "Non-payment by the Insured Entity of Insurance Premiums to the State Non-budgetary Fund for Compulsory Social Insurance against Industrial Accidents and Occupational Diseases."

Deception as a way of committing fraud involving the receipt of payments covered by Art. 159.2 of the Criminal Code of the Russian Federation is defined as a submission to executive authorities, institutions or organizations authorized to make decisions on the issuance of payments, of knowingly false and (or) inaccurate information about the existence of circumstances whose occurrence, according to the law or applicable regulations, constitutes a prerequisite for the issuance of corresponding payments in the form of cash or other assets (in particular, about the recipient's identity, disability, children, dependents, participation in hostilities or lack of employment opportunities), as well as the withholding of information about the loss of eligibility to receive these payments. If a person, by providing deliberately false and (or) inaccurate information or by omitting important facts, manages to obtain a document certifying his eligibility to receive social benefits, but, due to circumstances beyond his control, does not actually use it to obtain the said social benefits, such person should be charged under Art. 30, part 1, of the Criminal Code with a preparation to commit fraud in order to obtain social benefits; provided, however, that the circumstances of the case prove that the person intended to use this document to commit offences falling under Art. 159.2, parts 3 and 4, of the Criminal Code of the Russian Federation[20].

Officials involved in the said criminal schemes, subject to the availability of supporting evidence, may be charged with offences falling under Art. 201 "Abuse of Authority," Art. 204 "Commercial Bribery," Art. 204.1 "Mediation in Commercial Bribery" Art. 285 "Abuse of Office," Art. 285.1 "Misappropriation of Public Funds," Art. 286 "Abuse of Public Authority" and Art. 290 "Acceptance of a Bribe" of the Criminal Code of the Russian Federation.

All above offences may be predicate to money laundering.

Types of fraud characteristic for the period of coronavirus pandemic

The global economic crisis caused by the coronavirus pandemic has triggered a wave of new types of fraud as well as an increase in the number of crimes committed online. Analysis of the available information, including from the FATF Secretariat, points to the higher risk of the following types of fraud during the coronavirus pandemic.

1. Fraud linked to the embezzlement of private and corporate funds allocated for the purchase of personal protective equipment and test systems for identification of counterfeit medicines and medical products, without actual delivery of the goods to the buyer

According to clarifications given in para. 3 of the Penal of the Supreme Court Resolution No. 48 "On judicial practice in proceedings involving fraud, misappropriation and embezzlement," persons committing such actions should be charged under Art. 159 of the Criminal Code "Fraud"; provided, however, that the person's intent to steal another person's property or acquire the right to it had existed prior to his receipt of the payment for goods, works or services he did not intend to provide/perform.

2. Supply of low-quality medical devices or other goods unsuitable for their intended use

According to clarifications given in para. 2-5 of the Penal of the Supreme Court Resolution No. 48 "On judicial practice in proceedings involving fraud, misappropriation and embezzlement," persons committing such actions may be charged under Art. 159 of the Criminal Code "Fraud."

[20] Paragraph 16 of the Plenum of the Supreme Court of the Russian Federation Resolution No. 48 dated 30 November 2017 "On judicial practice in proceedings involving fraud, misappropriation and embezzlement"

The embezzlement in this case is committed through deception: a deliberate communication of deliberately false or inaccurate information, omission of facts, or deliberate actions (e.g. the provision of fake goods or other contractual items) aimed at misleading the owner of the property or another person[21].

3. Embezzlement of private or corporate funds committed under the guise of charitable fundraising (to help COVID-19 patients, their family members, medical workers, etc.). Typically, criminals post their fundraising appeals on instant messenger and social media platforms. These actions may constitute offences falling under Art.159 "Fraud" of the Criminal Code[22].

Raised funds may be used, among others, for terrorist and proliferation financing. Persons raising funds for TF under the guise of anti-COVID-19 efforts or relief for the infected may be charged with offences falling under Art. 205.1, part 4, "Organizing Terrorist Financing" of the Criminal Code of the Russian Federation.

Persons donating funds for the above causes while being aware of their intended use for terrorist financing purposes should be charged with offences covered by Art. 205.1, part 1.1. "Terrorist Financing" of the Criminal Code of the Russian Federation. If raised funds were intended to finance an illegal armed group, such actions constitute offences falling under Art.208, part 1, "Financing of an Illegal Armed Group."

4. Sales of drugs or vaccines presumably effective against COVID-19

Despite the absence of officially recognized vaccines, the first ads promoting COVID-19 remedies appeared on the Internet as early as January 2020. In addition, online venders sell anti-COVID-19 amulets, potions and religious items, as well as offer various occult services such as enchantments, spells and sale of "charmed water," etc. that claim to provide immunity against the coronavirus.

According to clarifications given in para. 2-5 of the Plenum of the Supreme Court of the Russian Federation Resolution No. 48 dated 30 November 2017 "On judicial practice in proceedings related to fraud, misappropriation and embezzlement," persons committing such actions may be charged with offences covered by Article 159 "Fraud," committed by deception or abuse of trust.

5. Mailing to private persons notices and messages containing demands for payment of fines for alleged violation of the self-quarantine regime

Such actions constitute offences falling under Art. 159 "Fraud" of the Criminal Code of the Russian Federation.

6. Mailing of letters to subscribers, including those purportedly sent by health care institutions or the World Health Organization, with messages on COVID-19 symptoms and consequences, that contain malicious software designed to steal personal data or payment details

According to clarifications given in par. 8 of the Penal of the Supreme Court Resolution No. 48 "On judicial practice in proceedings involving fraud, misappropriation and embezzlement," such actions, depending on the object of the offence and other circumstances of the case, meet the definition of fraud and as such are covered by Art. 159, Art. 159.3 "Wire Payment Fraud" and Art. 159.6 "Computer Data Fraud" of the Criminal Code of the Russian Federation.

7. Solicitation of money from individuals by fraudsters posing as their COVID-19 sick relatives or hospital staff According to clarifications given in para. 2-5 of the Plenum of the Supreme Court of the Russian Federation Resolution No. 48 dated 30 November 2017 "On judicial practice in proceedings related to fraud, misappropriation and embezzlement," persons committing such actions may be charged with

[21] Paragraph 2 of the Plenum of the Supreme Court of the Russian Federation Resolution No. 48 dated 30 November 2017 "On judicial practice in proceedings involving fraud, misappropriation and embezzlement"

[22] Paragraph 3 of the Plenum of the Supreme Court of the Russian Federation Resolution No. 48 dated 30 November 2017 "On judicial practice in proceedings involving fraud, misappropriation and embezzlement"

offences covered by Article 159 "Fraud" of the Criminal Code of the Russian Federation, committed by deception or abuse of trust.

8. Sale of COVID-19 free passes during self-isolation regime, including to persons quarantined due to COVID-19 infection or contact with the infected. Such actions constitute offences falling under Art. 159 "Fraud" of the Criminal Code of the Russian Federation, committed by deception or abuse of trust.

All above offences may be predicate to money laundering.

As it stands, the majority of crimes involving the embezzlement of public funds and corruption remain undetected long after they have been committed. In this regard, failure to register offences linked to the above risks does not imply their absence.

To combat the public funds embezzlement, we should make the monitoring of funds allocated for COVID-19 relief and in support of businesses affected by the pandemic one of our top priorities for the immediate future.

NATIONAL AML/CFT SYSTEM

ROSFINMONITORING PUBLISHES ANNUAL REPORT 2019

The Federal Financial Monitoring Service has posted its Annual Report 2019 on its official website. "Financial Security" publishes its key results

In 2019, Russia in the framework of the 4th round of the FATF mutual evaluations was assessed by the Financial Action Task Force (FATF), the Council of Europe's Committee of Experts on the Evaluation of Measures against Money Laundering and the Financing of Terrorism (MONEYVAL), and the Eurasian Group on Combating Money Laundering and Financing of Terrorism (EAG).

Following the completion of the assessment and adoption of the final report by the FATF Plenary on October 17, 2019, the Russian Federation was placed in the regular follow-up process (the best possible result under the existing procedures), with the follow-up report on the elimination of the identified deficiencies due in 3 years.

With respect to the **formulation of the state policy and regulatory framework,** Rosfinmonitoring has amended the country's AML/CFT regulations. The most important, among them, was Presidential Decree No. 289 dated June 24, 2019 "On amendments to Presidential Decree No. 808 dated June 13, 2012 'Matters concerning the Federal Financial Monitoring Service' and the Regulation adopted by this Decree," which empowered Rosfinmonitoring to develop ML/TF risk mitigation and prevention measures.

With respect to international cooperation, Rosfinmonitoring's priories for 2019 were as follows:

- maintaining compliance of Russia's AML/CFT system with international requirements;
- making Russia's involvement in international AML/CFT/CPF efforts more active;
- improving the effectiveness of international AML/CFT institutions.

Customarily, much attention in this area was devoted to **cooperation with foreign financial intelligence units,** particularly in identifying and seizing stolen assets abroad and providing assistance to investigative authorities.

Rosfinmonitoring's involvement in investigations carried out by the Investigative Committee, FSB and the Ministry of Internal Affairs into the embezzlement of Probusinessbank's assets contributed to the detection and immediate freezing of assets totalling more than US 140 million.

In 2019, Rosfinmonitoring, in collaboration with the General Prosecutor's Office, the Ministry of Internal Affairs, the Investigative Committee, FSB, FCS and FTS, identified and forwarded relevant documents for further seizure and return to Russia of assets totalling RUR 50 billion.

To strengthen bilateral AML/CFT/CPF cooperation, Rosfinmonitoring and the International Training and Methodology Centre for Financial Monitoring (ITMCFM) provided technical assistance to partner countries.

In the framework of the EAG, chaired by Russia, the following assistance was provided:

- in training (at ITMCFM, International Network Institute, etc.) and upgrading the skills of personnel;
- in organizing various events (workshops, trainings, etc.);
- in undergoing mutual evaluations.

In 2019, Rosfinmonitoring and other domestic AML/CFT stakeholders worked to **mitigate the risks** identified in the National ML/TF Risk Assessment (NRA).

The following areas were identified as high risk:

- the financial sector,
- corruption offences,
- budget relations,
- drug trafficking,
- terrorist financing.

Measures taken by Rosfinmonitoring, the Bank of Russia and law enforcement agencies in the financial sector helped reduce the volume of suspicious transactions by more than 40 percent, as well as diminish the number of cash-out transactions by 45% and decrease the overall volume of funds moved out of the country on dubious grounds.

As part of the Bank of Russia's financial sector clean-up, 31 banks lost their licenses in 2019; in 80 percent of cases Rosfinmonitoring in advance informed BoR on the financial institution's involvement in suspicious transactions.

Thanks to the efforts undertaken by Rosfinmonitoring in collaboration with FTS, the Bank of Russia and AML/CFT stakeholders, the number of identified shell companies has fallen to a new low of 120,000, with the total volume of transfers to their accounts falling twofold.

In the sectors supervised by Rosfinmonitoring in 2019, the use of remote communication tools, i.e. Personal accounts, as well as the adoption of measures designed to raise reporting entities' awareness of legal requirements and the results of national and sectoral risk assessments, resulted in a 3.5 percent increase in compliance with legal requirements, including among leasing and factoring companies.

Preventive measures taken by banks, particularly denial of service to unscrupulous clients, quite effectively contributed to the curbing of shadow economy. The application of prohibitive measures helped prevent more than RUR 200 billion from entering the shadow sector in 2019.

Meanwhile, the year-over-year decline in the number of service denials by banks suggests not only a decrease in the number of illegal transactions in the economy, but also a more balanced and responsible fulfillment by both banks and their clients of legal requirements.

As part of the efforts to decriminalize the financial sector, Rosfinmonitoring, jointly with the Bank of Russia, FSB, the Ministry of Internal Affairs, the Investigative Committee, FTS and the General Prosecutor's Office, in 2019 shut down 25 illicit financial platforms specializing in cashing out and transferring the money abroad, putting an end to operations worth RUR 40 billion.

In total, Rosfinmonitoring's intelligence was used in 2019 to launch 700 criminal investigations into offences committed in the financial sector, with 168 reaching court, including 107 resulting in convictions. The total amount of recovered funds is estimated at RUR 50 billion. Nevertheless, unscrupulous market participants continue to misuse the country's financial system for ML purposes.

Rosfinmonitoring works on an ongoing basis to combat corruption-related money laundering.

Work is also underway to mitigate the risks associated with bribes paid to officials who abuse their office to help unscrupulous suppliers and contractors to win government contracts.

A total of 80 criminal investigations were launched and completed in 2019 using the intelligence provided by Rosfinmonitoring. According to FSB information, in 2019 it successfully investigated crimes committed by 4 heads of constituent entities, 13 deputy governors, 22 regional officials and 40 heads of municipalities. Analytical materials provided to law enforcement contributed to the removal from office, arrest and conviction of a number of high-ranking civil servants and employees of state-owned companies.

As part of its efforts to monitor public procurement, Rosfinmonitoring scrutinized transactions carried out by both contractors at the stage of the contract implementation and procurement participants during the bidding process. One of the priorities is to identify possible collusion of bidders both with each other and customers, which creates conditions for the overstatement of the value of government contracts and the subsequent embezzlement of public funds.

Rosfinmonitoring also **monitors the expenditure of public funds allocated for national projects** implemented in accordance with Presidential Decree No. 204 dated May 7, 2018 "On national goals and strategic objectives of the Russian Federation up to 2024."

As part of its efforts in this area, Rosfinmonitoring monitored suspicious transactions carried out by 22,000 contractors working on national contracts totalling RUR 160 billion. As a result of this work, over 740 financial investigation findings linked to national projects were passed on to law enforcement, supervisors and the General Prosecutor's Office, resulting in 13 criminal investigations with incurred damages in excess of RUR 1.8 billion, as well as in the termination of contacts and cancellation of procurement orders totalling RUR 1.2 billion. Investigators also uncovered cartel agreements worth RUR 2.8 billion linked to the "Education" and "Housing and Urban Environment" national projects, with the amount of recovered damages estimated at RUR 7.5 million.

The results achieved by the **existing defence procurement oversight system** highlight the overall success of the efforts to decriminalize the sector and improve its transparency, i.e.:

- The number of cooperation sector participants making dubious transactions has decreased almost 1.5-fold, with the total amount of such transactions falling by more than threefold;
- the number of suspicious defence contractors has decreased by more than 30%;
- the number of refusals to carry out transactions issued to defence contractors on informal grounds has fallen almost twofold.

107 criminal proceedings into defence procurement-related violations were initiated in 2019, with damages totalling over RUR 13.5 billion and prevented embezzlement estimated at RUR 2.8 billion. At the same time, the total amount of funds recovered with the help of Rosfinmonitoring's intelligence amounted to RUR 5.4 billion.

To **decriminalize certain socially significant areas and sectors of the real economy,** as well as to counter corruption and mitigate relevant risks, Rosfinmonitoring conducts a comprehensive monitoring of individual sectors and projects.

This work includes the **protection of the rights of private investors in shared equity construction projects.** As part of these efforts, Rosfinmonitoring conducted more than 320 inspections, including those initiated by interagency working groups under the Ministry of Construction of Russia and the General Prosecutor's Office, targeting over 1700 legal entities and 900 individuals. More than 500 findings generated by this process were forwarded to law enforcement

and used to initiate 400 criminal proceedings, with 60 reaching court and 20 resulting in convictions. The total amount of recovered damages is estimated at RUR 750 million.

Rosfinmonitoring's inspections were aimed at identifying financial transactions related to the embezzlement and subsequent legalization of funds, recovery of stolen assets, and prevention of future embezzlements.

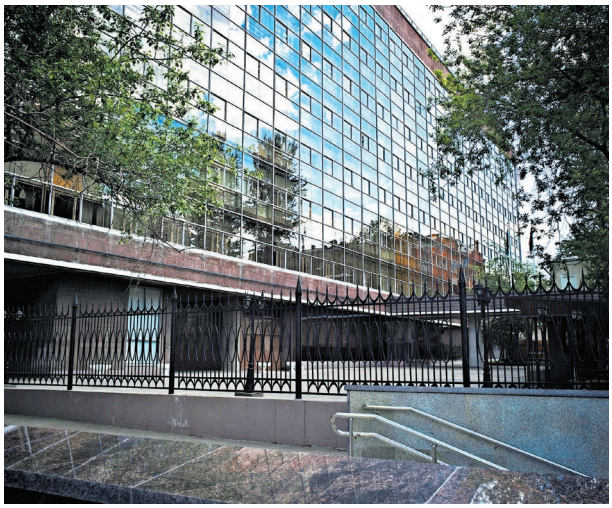
The slowing pace of bankruptcies regarding developers, recorded in late 2019, and unfinished projects point to a gradual decriminalization of the shared equity construction sector. This was made possible, among others, through the joint work of Rosfinmonitoring and other agencies, including the entry into force of amendments to the legislation and the gradual transition of developers to escrow accounts.

Rosfinmonitoring also worked hard to decriminalize the energy, housing, timber, fisheries and agricultural sectors.

For example, the purpose of the Melioration project, being carried out by Rosfinmonitoring, is to monitor the expenditure of funds allocated for the relevant federal target programs and national projects. The monitoring findings revealed that about 15 percent of these funds were transferred to the shadow economy from the accounts of melio-water enterprises and agricultural producers on fictitious grounds, with 36 percent of all melio-water enterprises engaging in corruption practices.

To tackle this problem, Rosfinmonitoring sent more than 60 disseminations to law enforcement. Rosfinmonitoring's intelligence was used to launch 14 criminal investigations into offences falling under Arts. 199, 159 and 159.2 of the Criminal Code, and 8 under Art. 174.1, resulting in the freezing of RUR 20 million and recovery of RUR damages in amount of RUR 102 million.

One of Rosfinmonitoring's strategic objectives is to prevent, identify and supress **trafficking in drugs and psychotropic substances.** To this end, the Russian FIU continuously improves its methods and approaches to the detection and recording of crimes related to drug trafficking committed with the use of modern information technologies.



Of 2500 inspections conducted by Rosfinmonitoring in 2019, more than 100 uncovered evidence of money laundering, with their findings being shared with law enforcement. Rosfinmonitoring's intelligence was used to initiate 150 criminal investigations into drug trafficking, including 80 into drug-related money laundering.

As part of the efforts to mitigate the **TF risk,** Rosfinmonitoring, in collaboration with law enforcement and the private sector, carried out more than 10,000 financial investigations, generating over 800 pieces of evidence used to launch 120 criminal investigations, including 65 TF investigations by FSB alone in relation to 64 persons, resulting in 20 convictions.

In collaboration with FSB, Rosfinmonitoring disrupted five major financing channels used by international terrorists to transfer RUR 120 million.

Rosfinmonitoring has stopped financial operations carried out by 4000 persons designated for terrorism and extremism, freezing RUR 36 million in their bank accounts.

Working in collaboration with the banking sector, Rosfinmonitoring identified over 260 persons suspected of being linked to terrorist financing.

Cooperation and coordination are key to an effective national AML/CFT system, with interagency cooperation being identified by the FATF as "the key strength of the Russian AML/CFT system."

Among those whose effectiveness was proven were the Interagency Working Group on Combating Illicit Transactions (IWG), chaired by Head of the Presidential Executive Office A. Vaino (and at the regional level under the leadership of plenipotentiary representatives of the President of the Russian Federation), the High-Level Interagency Commission (IC), AML/CFT/CPF IC, and IC on Combating Terrorist Financing.

High-Level IC showed its effectiveness in preparation process of Russia for the FATF 4th round of mutual evaluations. IC not only discussed most urgent issues of the evaluation process, but also became venue for work with experts from the agencies represented at the High-Level IC, who took part in face-to-face meetings with the FATF experts during the on-site visit, as well in discussion and adoption process of the Russian report on the international scene.

President of the Russian Federation Vladimir Putin expressed his support for Rosfinmonitoring's proposal to transform the High-Level IC on Preparation of Russia for the FATF 4th Round of Mutual Evaluations into Interagency Commission on Implementation of Measures to Improve the AML/CFT System Based on the Evaluation Findings.

At present, Rosfinmonitoring has prepared a draft interagency roadmap to eliminate the deficiencies identified during the evaluation procedure. Its purpose is to conduct a comprehensive assessment of all components of the Russian AML/CFT system.

The full version of the Annual Report is accessible via the “Activities” section on Rosfinmonitoring's official website.

ITMCFM: 2019 RESULTS

Excerpts from the International Training and Methodology Centre for Financial Monitoring official performance report

EXPERT CENTRE

Research Function

In 2019, ITMCFM introduced 11 research projects into AML/CFT specialists' training and practical activities expecially:

- when organizing 7 training courses and more than 25 workshops, including via video conferencing;
- during development of 2 AML/CFT training programs for INI participants;
- in the course of publishing 1 textbook and 1 training manual.

In 2020, ITMCFM plans to develop an architecture platform for ITMCFM training courses and test it on the basis of modular training course "Implementation of International AML/CFT Standards."

Methodological Function

ITMCFM on the basis of International Network Institute updates and launches specialized programs and higher education profiles incorporating vocational standard “Financial Monitoring Specialist in AML/CFT sphere”, updated educational standards, NRA and mutual evaluation findings, and also develops teaching aids.

ITMCFM, jointly with the All-Russian Academy of Foreign Trade (AAFT), the Karaganda State University (KarSU) and the Kyrgyz-Russian Slavic University (KRSU), have developed the training program

"AML/CFT and Legal Support of Economic Security" for KarSU, training program "Risk Analysis and Financial Monitoring" for KRSU, and training manual "Specifics of AML/CFT Systems of Eurasian Countries."

The outcomes of the joint ITMCFM/Kazakhstan/Kyrgyzstan project to elaborate relevant country sections of the training manual were presented to the EAG 30th Plenary and praised by the participants, who expressed their interest in continuing the implementation of this project with the participation of INI universities under the leadership of national FIUs.

ITMCFM also assisted in the preparation and publication of the first textbook, which is based on the country section of the training manual.

The AML/CFT Training and Research Advisory Board (TRAB), comprising representatives of the Presidential Executive Office, Rosfinmonitoring, the Ministry of Education and Science, the Bank of Russia, the Ministry of Internal Affairs, FSB, the Investigative Committee, ITMCFM, the Russian Academy of Sciences (RAS), and INI universities, was established within the structure of the Interagency AML/CFT/CPF Commission to improve cooperation among public authorities, the business community, universities and research centres in the training of AML/CFT personnel for Russia.

Personnel Function

In 2019, for the first time, separate trainings were organized for experts from the law enforcement and supervisory block. Supervisors participating in the workshop organized for EAG assessors (Kazan, Russia) took part in an evaluation simulation exercise and improved their practical skills in carrying out ME and preparing MERs.

Meanwhile, law enforcement officials participating in the assessors' training (Tashkent, Uzbekistan) learned from international experts with on-site assessment experience the practical aspects of the assessment process. The training included interviews with representatives of the assessed country (on-site visit), as well as the preparation and presentation of a mutual evaluation report.

The CPF training for EAG AML/CFT personnel (Moscow, Russia), built around the joint EAG/FATFTRAIN/ITMCFM program, focused on the latest trends and risks. Participants took part in a simulation exercise involving the adoption of a new CPF law in a fictional country and requiring the elaboration of national coordination mechanisms.

Such events help strengthen cooperation between EAG countries in confronting the global challenges of the 21st century.

Project Function

In 2019, ITMCFM modified its approach to TA prioritization by focusing on the results of mutual evaluations, the development and implementation of a country project, and assessment of its effectiveness.

In providing TA, the Centre focuses on identifying the hierarchy of the partner countries' TA needs according to the EAG priorities. The strategic objectives of TA provision lies in facilitating compliance of national AML/CFT systems with the FATF standards and in bringing of EAG member states' national AML/CFT systems closer together.

BASIC TRAINING INSTITUTION

Methodical Function

In 2019, the training course "Professional Development of AML/CFT Personnel" was conducted under an advanced program. Its main goal was to expand the knowledge acquired during the basic course and apply it in practice.

The focus of the advanced course was on the study of NRA techniques and familiarization with its findings, as well as on the experience of undergoing FATF and EAG mutual evaluation procedures.

INI universities' advanced teacher training program was expanded to include international cooperation workshops and round tables dedicated to the training of AML/CFT personnel for Eurasian region. Alongside teachers, participants of the above events included representatives of the Kyrgyz and Uzbek embassies, the EAG Secretariat and Rosfinmonitoring.

Analysis of participants' feedback highlighted the effectiveness and usefulness of the course from a practical standpoint, as well as its ability to contribute to the acquisition of new knowledge and its use in the organization of the educational process by university teachers.

Training Function

In 2019, Rosfinmonitoring experts attended the "Financial Intelligence and AML/CFT" training course, organized by ITMCFM and designed to help its participants to improve their skills and study international experience.

Training organized for supervisors included review of the preliminary results of the mutual evaluation of the Russian AML/CFT system and the steps taken to prepare for it. Supervisors familiarized themselves with the NRA key findings as well as with the capabilities and functionality of the supervisor's Personal account on the Rosfinmonitoring website.

To strengthen cooperation among national AML/CFT stakeholders, ITMCFM organized AML trainings for the staff of the Investigative Committee, FSB and

the Ministry of Internal Affairs. During their visits to the Centre, law enforcement personnel and investigators attended trainings on ML schemes and threats as well as on opportunities offered by international cooperation.

The Centre, with the expert support of Rosfinmonitoring, annually conducts anti-drug trainings for the employees of the Ministry of Internal Affairs Chief Drug Control Directorate.

In line with the 2019-2021 Comprehensive Interagency Action Plan to Combat the Financing of Terrorism and Extremism, ITMCFM provides trainings for employees of the Ministry of Internal Affairs and FSB.

The findings of the joint FATF/UNODC study "Detecting and Blocking of Financial Flows Linked to Illicit Traffic in Opiates" (2014), undertaken within the framework of the Paris Pact Initiative (UNODC), were used to designate the Balkans as a region at higher risk of being used for drug transit purposes. In view of Russia's role in MONEYVAL, UNODC proposed ITMCFM to implement the regional program on Enhancing the Capacity of Financial Intelligence and Law Enforcement Agencies of South-Eastern Europe in Conducting Financial Transaction Analysis and Investigations. The purpose of the program is to combat drug trafficking, terrorist financing and organized crime in the region, as well as to detect the cash flows underpinning the drug trade.

In 2019, ITMCFM organized a training on combating terrorism and extremism financing, attended by law enforcement and FIU officials from Albania, Bosnia and Herzegovina, Montenegro, North Macedonia, Serbia and Croatia.

The EAG 21st Plenary, by its decision dated November 2014, granted the CIS ATC observer status in the EAG.

The annual workshop on Upgrading the Skills of Law Enforcement Personnel in Combating Terrorist and Extremist Financing, held jointly by ITMCFM and CIS ATC since 2015 to study new TF schemes. In the framework of the workshop held in 2019 Russia's risk assessment approaches and mechanisms to detect TF transactions were presented.

The joint NDB/EAG/ITMCFM workshop on Improving AML/CFT Efforts by using New Technologies was held in Moscow in May 2019. The purpose of the workshop was to assist state authorities in understanding and developing regulatory and supervisory response measures to the use of virtual assets. ITMCFM and the New Development Bank (NDB), which acted as program developers and section moderators, invited key experts to attend the event.

Participants of the 5th international workshop on Public-Private Partnership to Strengthen AML/CFT Efforts, as well as consultations with the private sector in Kazan in 2019, discussed the effectiveness of preventive measures, the quality of suspicious transaction reporting, the application of targeted financial sanctions, best practices of AML/CFT cooperation with the private sector, innovative approaches and solutions to the issues concerning automation and the use of digital technologies for AML/CFT supervision, as well as international AML/CFT trends.

The event was attended by more than 130 representatives of FIUs and supervisory authorities, leading experts of the financial and non-financial institutions compliance departments of the EAG member and observer states, as well as representatives of the EAG Secretariat and ITMCFM.

The simulation exercise held during the workshop helped participants to develop a procedure for conducting a sectoral risk assessment for financial institutions and formulate proposals related to the establishment of an International Compliance Council (based on the experience of operation of the Russian Compliance Council).

To strengthen cooperation between the Russian Federation and other FATF and FSRB members, carried out in accordance with bilateral agreements, ITMCFM, on an annual basis, organizes AML/CFT personnel trainings for Russia's partner states. Their content is discussed in advance with the FIUs of the countries involved, and include topics that take into account the interests and needs of students.

In 2019, the training course program included topical issues covering the implementation of the FATF Recommendations (11 Immediate Outcomes, as well as the preparation and implementation of NRAs

and mutual evaluations). Participants took part in simulation exercises spanning such themes as "ML Identification and Investigation," "Understanding and Identification of ML/TF risks" and "TF Identification and Investigation"

29 AML/CFT experts from Azerbaijan, Belarus, Brazil, Vietnam, India, Iraq, Iran, Kazakhstan, Kyrgyzstan, Laos and Uzbekistan took part in three training courses.

INTERNATIONAL NETWORK AML/CFT INSTITUTE COORDINATOR

Academic Function

In 2019, the following subdivisions began their work at INI universities with support from ITMCFM:

- Financial Monitoring Training and Research Centre and the Financial Monitoring Department (RUDN, Moscow);
- Student Financial Intelligence Laboratory (MEPhI, Moscow);
- Research laboratory "Financial and Economic Security and Digital Transformation"(SFU, Krasnoyarsk).

Among the outcomes of the work carried out by INI expert departments, centres and laboratories was the updating and launch of new programs and higher education specialties based on the vocational standard for AML/CFT personnel, federal standards, and NRA and ME findings.

Interest in these programs is growing both in Russia and abroad: in 2019, 1,100 Russian students and 125 foreign nationals were admitted to study at INI.

Educational Function

In 2019, ITMCFM, together with INI training and research centres, as part of the efforts to improve the financial literacy of students, organized several lectures and master classes.

Practice-oriented Function

The INI 5th anniversary conference "AML/CFT in the Global World: Risks and Threats Facing the World Economy," attended by approx. 500 representatives from more than 20 countries, was held in 2019. Among the main topics of the conference were AML/CFT in the digital era, AML/CFT-related artificial intelligence, the nature of risks and threats in the global economy, and the digital transformation of the AML/CFT educational space.

INFORMATION CENTRE

Service Function

In 2018, the CIS Council of Heads of FIUs approved the project of Information Sharing System (ISS), whose purpose is to build a secure information-sharing network in Eurasia.

The Secure Network Management Centre (NMC) was established on ITMCFM platform, with subscriber nodes in Russia, Kyrgyzstan, Kazakhstan and Tajikistan. To date, it has been used to exchange information between the Russian and Kyrgyz FIUs.

Pursuant to the EAG 29th EAG Plenary Decision dated November 2018, ITMCFM provides technical assistance to Kyrgyzstan in several areas, with a focus on creating a specialized module "Entity's Personal account on the official website of the State Financial Intelligence Service under the Government of the Kyrgyz Republic."

In 2019, the first phase of the project to build a Personal account was completed, which included its design and a project model.

Starting in 2013, ITMCFM began to make daily reviews of AML/CFT/CPF media publications, followed, in 2019, by daily reviews of Russian media publications, weekly reviews on strategic enterprises, the effects of the FATCA law, monthly reviews of foreign media publications, as well as thematic reviews made in response to requests received from various FIU departments.

Since its establishment in 2005, ITMCFM has been translating into Russian the official documents of the FATF, FSRBs and Egmont Group for their distribution within Eurasia. ITMCFM is authorized by FATF to publish and distribute the translated versions of its documents.

In 2019, a large proportion of translation work was linked to the mutual evaluation of Russia by the FATF.

A team of simultaneous interpreters have been cooperating with ITMCFM since 2007. In 2019, over 900 hours, or more than 120 business days, of translation services were provided at various events. A team of simultaneous interpreters provided translation services at FATF, EAG, MONEYVAL, Egmont Group, CHFIU, and BRICS AML/CFT Council meetings, INI events, training workshops and multilateral meetings.

Telecommunication Function

ITMCFM continues the publication of its periodicals: the "Financial Security" journal and the EAG Newsletter. Available in both Russian and English, the publications cover the latest AML/CFT/CPF developments.

Methodical Function

E-learning represents the latest trend in education, including in AML/CFT system. To improve performance of AML/CFT personnel, ITMCFM filmed in 2019 a series of videos that are available via the Rosfinmonitoring official website.

Coordination Function

Since 2009 a network of ITMCFM's partner educational institutions has been operating, which annually trains more than 30,000 employees of organizations carrying out transactions with funds and other assets.

In 2019, ITMCFM entered into 91 cooperation agreements with educational institutions, including multidisciplinary training centres, educational institutions providing services to various entities covered by AML/CFT legislation, and universities.

NATIONAL PROJECTS ARE THE MAIN STRATEGIC AREAS OF MONITORING AND CONTROL OVER BUDGETARY SPHERE

The meeting of Rosfinmonitoring's Collegium took place

A Collegium meeting entitled **"Monitoring of government expenditures, including funds allocated for the implementation of Russia's national projects. Challenges, solutions and opportunities for improvement" was held at the Federal Financial Monitoring Service on 24 July 2020.**

The meeting was attended by Deputy Chairman of the Federation Council of the Russian Federation N. Zhuravlev, Head of the Federal Treasury R. Artyukhin, Deputy Head of the Federal Tax Service K. Chekmyshev, State Secretary – Deputy Head of the Federal Antimonopoly Service A. Tsarikovsky, as well as representatives of the Presidential Executive Office, the General Prosecutor's Office, the Ministry of Internal Affairs, the Federal Security Service and the Bank of Russia.

In his welcoming remarks to the participants, **Director of Rosfinmonitoring, Yu. Chikhanchin,** noted that although efforts to build a system of state financial control over public spending in Russia had been made for almost 20 years, it was not until 2016, when the President of Russia signed amendments to the Law "On State Defence Procurement," putting in place public spending monitoring system, that the situation began to change for the better.

"The National Risk Assessment and the National AML/CFT System Development Concept identify budgetary sphere as one of the most vulnerable risk areas," said Yu. Chikhanchin. *"The main elements of the system are legislative, preventive and suppressive measures. As for rulemaking, we work closely with the Federation Council and the State Duma to introduce well-established mechanisms for budget monitoring. Meanwhile, the integrated application of preventive and suppressive measures allows us today to implement the "end-to-end" oversight of government expenditures at the same time reducing the administrative burden on contractors. The role played by the Risk Assessment Centre and Personal Internet Accounts in these efforts is invaluable."*

The head of the Russian financial intelligence unit reminded participants of the significant number of successful efforts to decriminalize the defence procurement sector and improve its fiscal transparency.

"We identified and disrupted numerous shadowy schemes used for carrying out pass-through and cash-out transactions. In addition we managed to prevent large losses of public funds," said the director of Rosfinmonitoring. "As instructed by the President of Russian Federation, the main strategic focus of oversight efforts in public sector should be, besides defence procurement, on national projects."

Enhanced support for projects throughout their entire life cycle (including control of final deliverables) is key to effective oversight of government expenditures. The choice of monitoring tools depends on the existing risk indicators and identified entity's vulnerabilities.

Considerable amount of funding allocated for national projects is channelled through regional administrations, which are tasked with addressing the majority of objectives related to the implementation of national projects set by the President of Russian Federation. Rosfinmonitoring's experience in implementing pilot projects to identify shadowy contracts at the regional level has been recognized by the Government of the Russian Federation as successful.

According to **Deputy Director of Rosfinmonitoring O. Krylov,** issues concerning monitoring of government spending have been the focus of Rosfinmonitoring's efforts right from the outset. *"The analytical report "Budget" – the first automatically compiled selection of suspicious financial transactions related to public funds – was completed 10 years ago,"* said Krylov. *This tool allowed to identify approximately 500 transactions requiring manual processing every day. Already back then, the Ministry of Internal Affairs and the Federal Security Service were making use, often quite successfully, of our spontaneous disseminations."*

O. Krylov noted that preventive and suppressive measures in the budget monitoring sector were among the focus areas of the FATF mutual evaluation, successfully completed by Russia in 2019. The system was highly rated by the FATF and played an important role in achieving this outcome, taking into account the unconventional and novel approach used in AML/CFT practice.

In his speech, Deputy Chairman of the Federation Council of the Russian Federation N. Zhuravlev said that Rosfinmonitoring had acquired the reputation of an agency capable of solving the problems professionally: *"The Federation Council places great emphasis on the implementation of national projects, especially at the regional level. Meanwhile, Rosfinmonitoring keeps detecting new financial schemes used by unscrupulous entities, some of which can only be dismantled with the help of legislative amendments. For its part, the Federation Council promptly reacts to legislative initiatives coming from Rosfinmonitoring."*

According to the **Head of the Federal Treasury R. Artyukhin**, *"Rosfinmonitoring takes the lead in establishing law and order in the public sector,"* as evidenced by joint results achieved in monitoring the implementation of national projects. *"This work can be used as a model for the overall government spending monitoring system,"* said R. Artyukhin. *"After all, it was Rosfinmonitoring who first placed the focus on traceability, i.e. use of codes, classifications and the ongoing monitoring of milestones along the entire cash flow. Following the results of H1 2020, we can all see that out of 95,500 contracts related to national projects, 28,000 are exposed to risk. So what can be done here? It means that the interagency cooperation mechanism must be expanded to cover the administrators of national projects."*

State Secretary – Deputy Head of Federal Antimonopoly Service A. Tsarikovsky admitted, *"All that has been said today means that all our agencies share common objectives. Recently, the Federal Antimonopoly Service, working jointly with Rosfinmonitoring and the Federal Security Service, has uncovered a scheme used by construction companies totalling RUR 5.6 billion. This is only one such case, but I have a feeling that it is just the beginning. Although much is being done now to combat COVID-19 pandemic, I have a premonition that in one year from now supervisors will have much work to do in this area."*

Deputy Head of the Federal Tax Service K. Chekmyshev: *"We consider Rosfinmonitoring our permanent strategic partner and ally in all challenges facing us. It is important that today we view the situation in a similar light; we see the entire scheme, rather than its separate components – from the beginning till the end."*

Among other issues discussed at the Collegium meeting were:

- The need for additional regulation of government expenditures;
- The development of a monitoring system;
- Mitigation of corruption risks in the public sector, etc.

Participants also welcomed the signing by Rosfinmonitoring of a supplementary agreement with the Russian Treasury, which expanded information sharing between the agencies: from now on, Rosfinmonitoring will notify the Treasury of any risk of failure or ineffective implementation of national projects identified by it.

INTERNATIONAL BLOCK

32ND EAG PLENARY MEETING – THE FIRST MEETING HELD BY THE FATF GLOBAL NETWORK AS A VIRTUAL EVENT

The meeting of the Eurasian Group on Combating Money Laundering and Financing of Terrorism (EAG) chaired by Director of Rosfinmonitoring, Yury Chikhanchin, was held remotely on June 19, 2020

In his welcome speech, Yury Chikhanchin expressed condolences for COVID-19 victims in the EAG member states and wished all coronavirus patients a speedy recovery.

The coronavirus has affected all aspects and spheres of life and is impacting the operation of the international AML/CFT platforms, including the EAG. This time our session does not include the meetings of the Working Groups and is held in the virtual mode, which has already been successfully tested by the FATF and other FSRBs.

The EAG Chairman pointed out that the Group, being the integral part of the FATF Global Network, bears the particular responsibility for ensuring financial security in the Eurasian region. In this context and in line with the EAG Strategy for the upcoming years, as well as with the priorities of the Russian Chairmanship, he underscored the need to focus the efforts on identification and mitigation of regional risks.

Yury Chikhanchin:

Another important aspect. Since we are focused on practical effect of the jointly taken measures implemented to address new challenges and threats in the financial sphere, I believe that it is necessary to ensure further rapprochement between the EAG and the Council of Heads of FIUs in terms of closer coordination of the important typology research and projects. The establishment of the international Risk Assessment Center should facilitate the achievement of this goal.

The FATF President Mr. Xiangmin Liu delivered a welcome speech and expressed the regret that the meeting could not be held in China due to the coronavirus that frustrated many plans. He noted that this Plenary is the first one held by the FATF Global Network as a virtual event, and the next one will be the FATF Plenary which will also be held in the virtual mode.

Mr. Xiangmin Liu:

COVID-19 did not affect our commitment to fight against money laundering, terrorist financing and financing of proliferation of weapons of mass destruction. As you know, about two weeks ago, the FATF published the basic document which reflected the FATF response to new challenges and threats caused by the pandemic. And the EAG also contributed to this study.

In his speech, the FATF President also summarized the results achieved during the Chinese Presidency of the FATF, the key priority of which was to strengthen the FATF Global Network.

The measures undertaken by the FATF and the EAG member states to mitigate the money laundering and terrorist financing risks caused by COVID-19 pandemic were among the key topics discussed at the meeting. The representatives of Uzbekistan and Rosfinmonitoring delivered presentation on this issue.

The Plenary emphasized the need for a rapid response to new ML/TF threats arising from the global pandemic. It was noted that the EAG member states work hard to identify and analyze new ML/TF methods in the region, assist in raising awareness among government authorities and the private sector of the latest global trends and emerging risks, as well as take active steps to bolster international cooperation in order to strengthen national AML/CFT systems.

Other issues of the meeting agenda included: the mutual evaluations of Turkmenistan and Uzbekistan (it was decided to postpone them due to the pandemic), and the engagement with the private sector, which becomes especially important in the context of the imposed restrictive measures. Besides that, the Plenary restored the Germany's status as the EAG observer.

The 33rd EAG Plenary Meeting is planned to be held in the Republic of Uzbekistan in November 2020 (in case of positive development of the global epidemiological situation).

FATF PLENARY: GERMANY'S PRESIDENCY STRATEGY AND GLOBAL NETWORK GENERAL TASKS

Due to the restrictions introduced in response to the COVID-19 pandemic, the FATF held its Plenary meeting via videoconferencing and it lasted longer than usual – from 8 to 24 June 2020. Russian Federation was represented by interagency delegation headed by Rosfinmonitoring and comprised of Ministry of Foreign Affairs, Federal Security Service, General Prosecutor's Office, Investigative Committee, Ministry of Finance, Federal Tax Service, Ministry of Internal Affairs and Bank of Russia

This Plenary was the last Plenary Meeting under the one-year Chinese Presidency represented by Mr. Xiangmin Liu of the People's Republic of China. During the Plenary Marcus Pleyer, the General Director of the German Federal Ministry of Finance, was elected as a new FATF President. Dr Pleyer's term will begin on 1 July 2020, and he will be the first FATF President with a two-year term in accordance with the recently revised FATF mandate.

Under the German Presidency, the FATF will continue its timely response to the COVID-19-related ML/TF offences commenced by the predecessors, identification of the parameters of the next round of the FATF mutual evaluations and implementation of the initiatives on asset recovery, beneficial ownership and combating the financing of proliferation of weapons of mass destruction (CPF).

According to Marcus Pleyer, the FATF will focus on introducing the potential of digital technologies in AML/CFT sphere, studying ML typologies related to environmental crimes, identifying the links between terrorist financing and illicit arms trafficking, and scrutinizing the financing of ethnically or racially motivated terrorism.

Marcus Pleyer, FATF President 2020-2022

The Plenary also elected Elisa de Anda Madrazo of Mexico's Ministry of Finance to the post of FATF Vice-President.

The Russian representative (Yulia Lafitskaya from Rosfinmonitoring) co-chaired the meeting of the key FATF Working Group - Policy Development Group (PDG).

The central topic discussed by the Plenary was the strategic review of the FATF key procedures and focus areas. Russian delegation was strongly in favour of maintaining existing principles of work based on tried-and-tested system. This system is characterised by impartiality and holistic approach and provides an opportunity for assessing all closely integrated elements of the national AML/CFT framework as a whole. This view is supported by the majority of the FATF member states, but discussions will continue in the intersession period and the results will determine next steps for optimisation of the FATF work.

Despite the spring 2020 decision to suspend evaluation procedures for 4 months due to COVID-19 pandemic, an exception was made for Iceland and Mongolia. Both countries have almost completed implementation of the action plan developed jointly with the FATF in order to eliminate strategic deficiencies of the national AML/CFT systems. These results made it possible to include the issue on the Plenary agenda and get “green light” for the earliest possible dispatch of on-site missions to Reykjavic and Ulaanbaatar to verify the achieved progress which is a necessary condition for exclusion from the “grey list”.

Participants expressed their support for the EAG's proposal to hold a joint FATF expert meeting in India, provisionally scheduled for November 2020.

The Plenary also adopted the FATF report for the G20 on so-called stablecoins, which, along with an overview of the revised FATF standards on virtual assets and virtual asset service providers, is accessible on the FATF website.

The next FATF Plenary is scheduled to take place this October in Paris, France.

COVID-19 AND MEASURES TO COMBAT ILLICIT FINANCING

Statement by the FATF President

As the global standard-setter for combating money laundering (ML) and the financing of terrorism (TF) and proliferation, the FATF encourages governments to work with financial institutions and other businesses to use the flexibility built into the risk-based approach to address the challenges posed by COVID-19 whilst remaining alert to new and emerging illicit finance risks. The FATF encourages the fullest use of responsible digital customer onboarding and delivery of digital financial services in light of social distancing measures. At a time when critical relief is needed in-country and beyond, effective implementation of the FATF Standards fosters greater transparency in financial transactions, which gives donors greater confidence that their support is reaching their intended beneficiaries. The continued implementation of the FATF Standards facilitates integrity and security of the global payments system during and after the pandemic through legitimate and transparent channels with appropriate levels of risk-based due diligence.

Addressing COVID-19-related financial crime risks by remaining vigilant

Criminals are taking advantage of the COVID-19 pandemic to carry out financial fraud and exploitation scams, including advertising and trafficking in counterfeit medicines, offering fraudulent investment opportunities, and engaging in phishing schemes that prey on virus-related fears. Malicious or fraudulent cybercrimes, fundraising for fake charities, and various medical scams targeting innocent victims are likely to increase, with criminals attempting to profit from the pandemic by exploiting people in urgent need of care and the goodwill of the general public and spreading misinformation about COVID-19. National authorities and international bodies are alerting citizens and businesses of these scams, which include impostor, investment and product scams, as well as insider trading in relation to COVID-19. Like criminals, terrorists may also exploit these opportunities to raise funds.

Supervisors, financial intelligence units and law enforcement agencies should continue to share information with the private sector to prioritize and address key ML risks, particularly those related to fraud, and TF risks linked to COVID-19. Additionally, criminals and terrorists may seek to exploit gaps and weaknesses in national anti-money laundering/ counter-financing of terrorism (AML/CFT) systems, making risk-based supervision and enforcement activity more critical than ever. Financial institutions and other businesses should remain vigilant to emerging ML and TF risks and ensure that they continue to effectively mitigate these risks and are able to detect and report suspicious activity.

Digital onboarding and simplified due diligence

With people around the world facing confinement or strict social distancing measures, in-person banking and access to other financial services is difficult, and unnecessarily exposes people to the risk of infection. Use of digital/contactless payments and digital onboarding reduce the risk of spreading the virus. As such, the use of financial technology (Fintech) provides significant opportunities to manage some of the issues presented by COVID-19. The FATF encourages the use of technology, including Fintech, Regtech and Suptech to the fullest extent possible. The FATF recently released Guidance on Digital ID, which highlights the benefits of trustworthy digital identity for improving the security, privacy and convenience of identifying people remotely for both onboarding and conducting transactions while also mitigating ML/TF risks. The FATF calls on countries to explore using digital identity, as appropriate, to aid financial transactions while managing ML/TF risks during this crisis.

When financial institutions or other businesses identify lower ML/TF risks, the FATF Standards allow them to take simplified due diligence measures. This approach may help them adapt to the current challenging situation. The FATF encourages countries and financial service providers to explore the appropriate use of simplified measures to facilitate the delivery of government benefits in response to the pandemic.

Delivery of aid

This global public health emergency has highlighted the vital work of charities and non-profit organizations (NPOs) to combat COVID-19 and its effects. The FATF has long recognized the vital importance of NPOs in providing crucial charitable services around the world, as well as the difficulties in providing that assistance to those in need. The FATF has worked closely with NPOs over the years to refine the FATF Standards to provide flexibility to ensure that charitable donations and activity can proceed expeditiously through legitimate and transparent channels and without disruption. It is important to recognize that FATF Standards do not require that all NPOs be considered high-risk and that financial transactions be suspended with all high-risk jurisdictions. The aim of the FATF Standards is to ensure that financial transactions are done through legitimate and transparent channels and money reaches its legitimate intended recipient, and the aim of the risk-based approach is to ensure that legitimate NPO activity is not unnecessarily delayed, disrupted or discouraged. The FATF encourages countries to work with relevant NPOs to ensure that much needed aid is getting to its intended recipients in a transparent manner.

Ongoing outreach and advice

Regulators, supervisors, financial intelligence units, law enforcement authorities and other relevant agencies can provide support, guidance and assistance for the private sector on how national AML/CFT laws and regulations will be applied during the current crisis. Such guidance can give financial institutions and other businesses reassurance that the authorities share their understanding of challenges and risks involved in the current situation, and of the appropriate actions to take. Authorities in some countries have already taken swift action and provided this type of advice. Mechanisms by which victims, financial institutions, and other businesses can report COVID-19 related fraud may be especially useful.

At the international level, the FATF is working with the Committee on Payment and Market Infrastructures and the World Bank and the International Monetary Fund to help ensure coordinated policy responses for the continued provision of critical payment services against the backdrop of the COVID-19 crisis. In addition, the FATF is working with its members and the FATF-Style Regional Bodies to identify and share good practices in response to common issues faced in many affected countries.

FATF's commitment to support efforts to address COVID-19 issues

The FATF welcomes feedback and stands ready to provide further guidance to support the current global efforts to tackle the COVID-19 crisis and its effects.

PARTICIPATION OF THE RUSSIAN FEDERATION IN MONEYVAL WORKING MEETINGS

The Russian delegation headed by Rosfinmonitoring and composed of the representatives of the Foreign Ministry, the Ministry of Internal Affairs, the Ministry of Finance, the General Prosecutor's Office, the Federal Security Service, the Federal Tax Service, the Investigative Committee and the Bank of Russia took part in the working meetings of the Council of Europe's Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL) held between June 30 and July 3, 2020

Due to the travel restrictions imposed in response to the spread of the COVID-19 pandemic, these meetings were, for the first time, held via video conferencing, which, however, did not affect the quality of discussions and outcomes. The amendments to the MONEYVAL procedures that allow for remote decision-making were adopted; the principles of conduct for assessors were approved; and the horizontal analysis of member states compliance with the effectiveness requirements in the course of CFT investigations (Immediate Outcome 9 of the FATF Methodology) was presented.

In furtherance of the MONEYVAL Strategy for 2020-2022, the issue related to resumption of typology research was given thorough consideration. In this context, it was proposed to the Council of Europe's Committee to launch, under the leadership of Russia (Rosfinmonitoring, Ministry of Interior's Drug Control Department and Lebedev Physical Institute of the Russian Academy of Sciences) and jointly with the Eurasian Group on Combating Money Laundering and Financing of Terrorism (EAG), a new research project named *"Misuse of Cryptocurrency Platforms for Laundering Illicit Drug Trafficking Proceeds"*.

Special attention at the meetings was paid to the overview of the COVID-19 impact on effectiveness of the member states' AML/CFT systems prepared and presented by the MONEYVAL Secretariat. Besides that, the information on the main threats to the financial systems of the European and the Eurasian Regions and on measures taken by the countries for mitigating the emerging risks was presented. Rosfinmonitoring's expert, Mrs. Pershina, delivered presentation on the Russian experience in the fight against financial crimes during the coronavirus pandemic.

The follow-up reports of Lithuania, Isle of Man, Ukraine and Czech Republic (that were placed in different follow-up processes) were delivered, and it was decided to continue the review of their progress at the next plenary meetings, one of which has already been scheduled for the mid of September, 2020.

This session was arranged under the direction of the new Executive Secretary of MONEYVAL, Igor Nebyvaev (the former Rosfinmonitoring's employee and the former EAG Executive Secretary), appointed by the Council of Europe in March 2020. The appointment received positive response from the participants.

A QUARTER OF A CENTURY IN PURSUIT OF DIRTY MONEY

Twenty five years ago, in June 1995, the Egmont Group – the global professional association of financial intelligence units – was established. The Group took its name from the Egmont-Arenberg Palace in Brussels where the first meeting of the relevant agencies of 14 countries was held. Since then, this informal association has evolved into the global network of financial intelligence units of 164 countries. Connection of FIUs to the Egmont Secure Web provides for prompt exchange of confidential information, improves effectiveness of financial investigations, and facilitates identification and mitigation of transnational threats and risks

Yury Korotky,
First Deputy Director of Rosfinmonitoring
Egmont Committee Member
Head of the Russian Delegation

Igor Alekseev,
Advisor to Director of Rosfinmonitoring

Russia obtained membership in the Egmont Group in June 2002, ten months after the adoption of the Federal Law on Combating Legalization (Laundering) of Criminal Proceeds, also known as Law 115-FZ, and just four months after the commencement of full-fledged operation of the national FIU – the Financial Monitoring Committee (today, Rosfinmonitoring).

Recognizing the importance of strengthening the global status of the international network of financial intelligence units and the need for developing the regional anti-money laundering and countering the financing of terrorism (AML/CFT) system in the Eurasian Region, Russia supported the establishment and admission to the Egmont Group of 11 FIUs of the former Soviet Union Republics between 2004 and 2019. Since 2015, Rosfinmonitoring experts have been appointed as the Egmont Group's regional representatives of Eurasian Region.

The 20th Egmont Group Plenary Meeting held in St. Petersburg in July 2012 significantly strengthened the status of Russia in the global financial intelligence units community. The Best Egmont Case Awards (BECA) won by Rosfinmonitoring in 2012 and 2017 proved the high professional skills of the Russian analysts. The judging panel noted the complication of the exposed fraud and money laundering schemes, large amount of the identified criminal assets, the extended cooperation with the foreign FIUs and the anti-corruption focus of the cases submitted by Rosfinmonitoring.

At present, Rosfinmonitoring is actively engaged in the Egmont Group's projects particularly relevant for Russia. The financial profiles of foreign terrorist fighters and the indicators of corruption-related suspicious transactions developed with the active involvement of the Russian representatives were of great help in identifying the relevant transactions. Rosfinmonitoring has launched the project on identification of professional money launderers, actively contributes to projects related to identification and disruption of large-scale cross-border money laundering schemes ("laundromats"), supports cooperation of FIUs with Fin-Tech companies, and facilitates more effective participation of FIUs in the asset recovery efforts.

In the rapidly changing environment, the Egmont Group focuses on building capacity of its members and enhancing effectiveness of their cooperation with each other and other global AML/CFT stakeholders. Extension of the scope of the FIUs activities and international collaboration with their involvement is the imperative of our times, and Rosfinmonitoring follows this trend.

One of the important initiatives pursued by Rosfinmonitoring in 2019 involves analysis of cross-border financial flows between Russia and foreign countries, *inter alia,* using the Egmont Group platform. Currently, the Russian FIU participates in two large-scale Egmont Group's projects. In particular, it participates in the work of the International Financial Intelligence Task Force on ABLV Bank. Apart from restoring the reputation by removing the label "Russian Laundromat", the proposal of Rosfinmonitoring was approved to set the issue related to identification of professional money launderers as one of the areas of the cooperative efforts pursued under this project. The similar work is conducted by the Laundromats Project Team established under the Information Exchange Working Group.

The information provided by Rosfinmonitoring resulted in initiation of 39 criminal proceedings just by the Latvian law enforcement agencies, and allowed for freezing the ABLV customers' assets worth EURO 241 million.

On September 16-19, 2019, the Rosfinmonitoring delegation led by Deputy Director of Rosfinmonitoring Oleg Krylov visited Estonia (Tallinn), where it met with the Head of the Estonian FIU Madis Reimand. Russian delegation included Igor Loskutov, head of Rosfinmonitoring's North-Western Federal District Interregional Department, representatives of Rosfinmonitoring Headquarters and its Interregional Department; the Estonian side was represented by the national criminal police and prosecutor's office.

The discussions at the meeting were dedicated to the cooperation between the two countries, the findings of the joint financial investigations, and the fourth round of the Financial Action Task Force (FATF) mutual evaluation process, which Russia underwent in 2019.

The meeting culminated in a joint commitment to improve effectiveness of cooperation between the financial intelligence units of Russia and Estonia.

Yury Chikhanchin:

In recent years, on the initiative of and in cooperation with the Russian financial intelligence unit, the law enforcement agencies **instituted over 30 criminal proceedings against** the Russian individuals who used the services of Laundromats and were involved in their operation in Russia. The licenses of **around 40 Russian banks** engaged in those schemes were revoked.

The project on identification of illegal cross-border financial flows has been launched under the auspices of the Egmont Group, with the **financial intelligence units of over 40 countries** participating in this work. **At least 20 financial intelligence units** have started their own investigations in respect of national banks suspected of establishing or being implicated in the operation of the Laundromats. Just in the framework of examining the operation of the Latvian ABLV Bank, Rosfinmonitoring cooperates with the **financial intelligence units of 18 countries.**

Excerpt from the presentation of the implementation progress of the National AML/CFT System Development Concept at the session of the Federation Council December 11, 2019

A working visit to Rosfinmonitoring by a delegation comprising of the representatives of the Moldova financial intelligence unit, led by its Director Vasile Charco, took place on 1 October 2019. The visitors were welcomed by Director of Rosfinmonitoring Yury Chikhanchin, Deputy Directors Oleg Krylov and Vladimir Glotov, and the officers of the Russian FIU and law enforcement agencies.

The purpose of the meeting was to discuss bilateral cooperation between the agencies in conducting financial investigations, including examination of the supposed money-laundering scheme through Moldova and Latvia which was named "the Laundromat" by the Organized Crime and Corruption Reporting Project (OCCRP).

The typology report is posted on the Egmont Group website

Besides that, in 2019, Rosfinmonitoring, along with the financial intelligence units of Israel, the Netherlands and Ukraine, took part in the Egmont Group typology research project on laundering the proceeds of corruption. The typology report is posted on the Egmont Group website.

In July 2019, the report concerning the outcomes of the research project on professional money launderers, initiated by the Russian FIU jointly with the colleagues from the Netherlands, was adopted in Hague.

COMPLIANCE COUNCIL

RIGHT TO REFUSE TO RENDER SERVICE TO CUSTOMER AS AN EFFECTIVE ML/TF RISK MITIGATION MECHANISM

Vladislav Poltavsky,
Deputy Chairman of Absolut Bank Board
Member of Regional Compliance Council in the Central Federal District

The trends observed in the recent years show that the financial monitoring priorities of banks have shifted towards the application of preventive measures in respect of customers suspected of carrying out money laundering (ML) related transactions. One of the effective preventive instruments is the right of credit institutions to refuse completion of customer's instruction to execute a transaction as provided for in Article 7 of Federal Law 115-FZ.

The mechanism of exercising by credit institutions of the right to refuse to execute customers' instructions in a situation, when credit institution personnel suspect that a transaction is carried out for money laundering or terrorist financing purposes, has been introduced relatively recently. However, along with the right of banks to refuse to enter into a bank (deposit) account agreement with a customer, this mechanism has already proved its effectiveness in dealing with unscrupulous customers. It should be noted that, in practice, credit institutions use such refusal right as an extreme measure, typically when a customer is unwilling to engage in meaningful dialogue with a credit institution for resolving the emerging issues. On the one hand, the gradual decline in number of such refusals may indicate that unscrupulous customers are being "cleaned out" from the financial sector. But, on the other hand, it may also be indicative of a more deep and thorough analysis of customers' activities conducted by credit institutions at the onboarding stage and in the process of maintaining business relationships which, in turn, enables them to avoid refusal of services on a purely formal basis.

For example, after in-depth review of customer activities at the onboarding stage, Absolut Bank conducts ongoing monitoring and analysis of transactions carried out by the customer. In particular, the Bank takes into consideration the specificities of the customers' business profiles, screens the counterparties against the available information sources, analyzes the number of personnel employed by corporate customers, assesses the amount of actually paid wages compared to those payable in the industry, and reviews consistency of the nature of transactions carried out by the customers with their actual business activities. Besides that, the Bank assesses the tax burden borne by the customers taking into account the applicable tax system and the amount of payable VAT depending on the sources of income and the nature of expenditures (input/output VAT). Furthermore, the service refusal mechanism intended for minimizing potential engagement with businesses operating in the shadow sector is obviously the effective measure that enables us to prevent involvement of credit institutions in carrying out dubious transactions of their customers.

Despite the relatively small number of such refusals, the general trend indicates that shadow businesses are still looking for a way out of this situation and make attempts to "migrate" to other banks, where possible. But, in some cases, such companies, on the contrary, strive to maintain business relationships with their banks and seek judicial protection. Therefore, the practical application of the refusal mechanism often leads to litigation between banks and their customers who still disagree with the legitimate measures taken by banks fully in line with the applicable legislation. However, according to the legislation it is a bank that has to prove that customer's transactions are complex or unusual and have no apparent economic or lawful purpose. Furthermore, soundness and sufficiency of the grounds for recognizing the suspicious nature of customer's transactions or possible application of a formal approach by a bank are assessed by courts. In view of the above, we must unfortunately admit that today the decisions passed by courts in relation to such cases are highly controversial, which demonstrates lack of a unified approach to application of the provisions of Federal Law 115-FZ and, in some cases, may be indicative of incompetence of certain authorities, including judicial authorities, in the AML/CFT area. In particular, when considering cases related to application of Federal Law 115-FZ, courts often take the side of the "affected" customers. This might be primarily due to the fact that a court initially perceives a customer as the "weaker party in the conflict" and considers the measures taken by a bank as infringement of the customer's rights. In this situation, courts often try to support customers by making judgments in their favor. After that, the parties submit numerous appeals to courts at different levels, including the Supreme Court. In such circumstances, an expert opinion of an independent third party, which is unaffiliated with both bank and customer, may be decisive for the judicial authorities. And the authorized AML/CFT agency may act in this capacity. There are many examples of such engagement by Rosfinmonitoring, one of which is presented below.

A customer came under scrutiny of the financial monitoring unit of the Bank after making several non-transparent payments, where a portion of funds was moved to the shadow economy. The Bank took certain measures in line with the guidelines of the Bank of Russia and Rosfinmonitoring, and requested the customer to provide a set of documents and information concerning those transactions. However, the customer failed to present the full set of the requested documents for substantiating the economic purpose of the transactions and, therefore, the Bank could not qualify the customer's activities as transparent and consistent with the common market practice. In those circumstances, the Bank exercised the rights provided for in Article 7 of Federal Law 115-FZ, namely: the right to refuse to execute the customer's instructions for carrying out transactions and the right to terminate the bank account agreement as a result of multiple refusals to carry out customer's transactions.

The corporate customer was repeatedly informed about its right to rehabilitate itself through the pre-trial process as provided for in Article 7(13.4) of Federal Law 115-FZ, but the customer refused to exercise this right and instead initiated multiple lawsuits against the Bank.

In the course of the legal proceedings that lasted for a long time, the courts of first instance did not always recognize the measures taken by the Bank as legitimate and, therefore, the Bank filed appeals and cassation complaints in support of its position. At one stage of the litigation, the court engaged in this process the officers of Rosfinmonitoring's Interregional Department in the Central Federal District, whose knowledge and experience undoubtedly facilitated the impartial hearing of this case in the higher court.

After considering the claim seeking invalidation of the actions taken by the Bank, the Arbitration Court of Moscow District resolved to uphold the decisions of the arbitration court of first instance and the resolutions of the court of appeal, according to which the refusal by the Bank to execute the customer's payment instructions was recognized substantiated and legitimate in line with the powers provided for in Article 7 of Federal Law 115-FZ. This also helped to win the lawsuit concerning the claim seeking invalidation of the unilateral termination by the Bank of the bank account agreement. Ultimately, the Bank terminated business relationships with that corporate customer that carried out dubious transactions through the account opened in the Bank.

This example of participation of Rosfinmonitoring's officers in consideration of legitimacy of actions taken by credit institutions for implementing the AML/CFT requirements clearly demonstrates the importance and relevance of the efforts undertaken by the authorized agency for pursuing the main goal of Federal Law 115-FZ, i.e. the creation and implementation of the mechanism for combating money laundering, terrorist financing and financing of proliferation of weapons of mass destruction. In this context, it is necessary to emphasize the role of the Regional compliance council in achieving the aforementioned goal, which, in the course of its work, develops specific recommendations, inter alia, for the banking community for practical application in the process of implementation of the internal control procedures for mitigating ML/TF risks.

AML/CFT CONTROL TECHNOLOGIES, OR WHAT ENTERPRENEURS SHOULD BE READY FOR IN 2020–2021

*Federal Law 115-FZ On **Anti-Money Laundering and Combating the Financing of Terrorism** is one of the most discussed in the business community. Even if some businesses were not brought to the orbit of this law, they have most certainly heard about it. A wave of account freezes several years ago raised many questions and debates. In 2019, the business community was ready for new challenges but did not encounter any major restrictions or significant changes. What has changed now and should the business community expect new "bracing up" in 2020?*

Galina Kuznetsova,
Compliance Director, Tinkoff Bank

In 2017-2018, many entrepreneurs faced "flood" of inquiries and restrictions imposed by banks implementing provisions of Federal Law 115-FZ, and some companies even had their accounts closed. Russia launched an active campaign against cash-out practices, putting an end to schemes that had been operating for years. This affected not only shell companies and firms specially established for cash-out purposes, but some honest entrepreneurs also fell under suspicion, so broad discussion ensued.

Every tsunami is merely a consequence of an earthquake. In the case of Federal Law 115-FZ, this wave of account freezes resulted from changes of the regulators' approaches to business transaction monitoring. The use of cash in shadow schemes is indicated as a high-level risk in the National Risk Assessment. Indeed, cash-out proceeds help businesses evade taxes, facilitate implementation of corrupt schemes and effect payments of dubious transactions, i.e. illicit proceeds are also concealed in cash payments.

Since 2003, Russia has been a member of the FATF – global organization, which develops unified international standards on combating money laundering and the financing of terrorism. The FATF regularly monitors compliance with these standards on a global scale, practically in every country. The FATF's high evaluation rating influences assessment of a country's investment climate indicating that this is an investment-friendly country compliant with universally accepted standards.

In the late 2000s, Russia underwent the FATF mutual evaluation, following which our country received detailed recommendations on compliance with global standards. Toward the mid-2010s, the Central Bank and Rosfinmonitoring developed them into specific regulatory recommendations, launching active AML/CFT efforts.

Banks were required to become actively involved in these efforts and independently detect illegal cash-out transactions and transit practices, otherwise, they risked getting labeled as institutions promoting illegal cash-out practices. Clients verifications followed, sometimes that was done in a rush, since all banks were required to take prompt action without delay. Customers engaged in illicit practices had to leave, while those operating in the "grey" area had to learn to work within the framework of law. This situation stirred a lot of discussions and concerns.

Technologies became another factor that played its part in this. Hi-tech banks will always have advantages, such as fast processes, in-depth data processing, and better service. Technologies also foster more stringent controls. Many banks have long since learned to verify customers and their transactions online, which also became one of the major causes of termination of business relationships with some clients. This happened because this became possible. As recently as 5 years ago, cash-out transactions were monitored offline after the transaction had been completed. There was time enough for suspicious customers to cash out and abandon the account. In recent years, however, the cash-out business has become much more transparent for banks, and transactions are now verified at the time of their execution. Banks now can see many (if not all) of the practices that had previously remained concealed. It looks like everything came out in a proper way: the government took active steps, and banks managed to implement them from the technical perspective.

In 2019, things were quiet for businesses as many proprietors switched to legitimate practices, and only those looking for new loopholes were placed under compliance monitoring. In 2019, banks calibrated processes and tested their compliance technologies. Banks learned how to conduct even more in-depth analysis of businesses without restricting their operations. The number of inquiries from banks decreased by several times. The same goes for restrictions of remote banking services.

Federal Law 115-FZ was not in the center of attention of the business community. Yet this does not mean that controls have been weakened. On the contrary, they have become even more advanced technologically and more accurate, whereas regulatory requirements have become even more stringent. The Central Bank and Rosfinmonitoring regularly report a decline in the volume of transactions that show indication of illegal cash-out practices: in 2019, the number of such transactions decreased by 1.9 times compared to 2018. The same result was reported in 2018 compared to a reduction of 1.6 times in 2017. The trend is quite obvious, and the regulators are not going to stop.

In the latter half of 2019, Russia underwent another FATF mutual evaluation, following which the regulators received new recommendations. In 2020-2021, we are going to see new requirements and new steps taken by regulators. However, this second wave of changes is expected to be much milder for the existing businesses.

There are also two reasons for this. First, all of the parties concerned have already adapted to the new reality. The regulators have formulated more clearly their expectations from banks. In its turn, banks have accurately fine-tuned their compliance check processes and formulated their own recommendations for entrepreneurs on how they can avoid restrictions. Banks have learned how to communicate with businesses and substantiate their inquiries and requirements. Most importantly, entrepreneurs are now aware that they may receive an inquiry and respond to it successfully without any harm to their operations.

The second reason stems from technologies. Banks are accumulating more and more information about customers. The existing scoring technologies make it possible to evaluate the customer's business more accurately at the onboarding stage. This mitigates risks for banks and significantly complicates illegal cash-out processes. We are now actively using machine learning technologies that automate specific stages of checks and enable analysts to evaluate the customers' business more accurately. Banks' approach to businesses is not just in terms of black and white. We can detect all shades of grey, but still help businesses implement their processes within the framework of law and leave the risk zone.

Banks are not the only ones to adopt modern technologies. The controlling authorities, Rosfinmonitoring, and the tax service are implementing new technologies at the same or faster pace. As a result, control will become more rigorous. Banks have already assumed the role of allies capable of closely evaluating customer transactions and possess enough expertise to recommend their customers to adjust their business processes in order to work successfully under the new conditions.

MITIGATING THE RISKS OF USING ENFORCED DEBT RECOVERY INSTRUMENTS IN MONEY LAUNDERING SCHEMES

A criminal scheme involving the use of execution orders to this day remains to a large extent technically hard to disrupt, since it operates within the legal framework and is being constantly evolved and adapted to effective internal control measures taken by banks. Every new modification of this scheme is created for specific unlawful purposes

Ludmila Sokolova,
Director of Financial Monitoring Department,
Bank Zenith PJSC

It all started with the so-called "Moldavian" scheme, more commonly known as "the Moldavian laundry" or "laundromat", which was used by fraudsters to transfer funds abroad in 2010-2014.

Shadow companies then developed a variety of schemes with the use of the infrastructure of the judicial system, court enforcement officers, notaries, and labor disputes committees in order to both transfer funds to claimers' bank accounts abroad and to conduct cash-out transactions.

Recently, due to the fact that banks have started charging customers who close their bank accounts a rather high commission as part of efforts aimed at anti-money laundering and combating the financing of terrorism (AML/CFT), a new variety of the scheme that uses court orders of a magistrate judge has emerged. Being targeted by bank in the framework of AML/CFT efforts, a customer whose registration lasts less than 6 months and who is not conducting any meaningful business activities usually realizes that he faces a high bank commission, so he uses this scheme to avoid paying it.

All of the above-mentioned typologies are still being used to some degree or other by unscrupulous business entities despite the growing effectiveness of internal control measures taken by banks, the development of banking technologies, the implementation of scoring processes, online monitoring of customers' transactions, improvements made by public authorities to AML/CFT services, and use of AML/CFT services provided by Russian and international companies, merely because banks do not have legal basis to refuse to process execution orders that have not been revoked in the prescribed manner or declared unlawful by a court.

In fact, whenever they encounter criminal schemes with the use of execution orders, banks face a dilemma related to the violation of either the Federal Law No. 115-FZ of August 7, 2001 *On Anti-Money Laundering and Combating the Financing of Terrorism* (hereinafter "Law No. 115-FZ") or the Federal Law No. 229-FZ of October 2, 2007 *On Executive Proceedings*.

Unreasonable refusal by a bank to comply with an execution order entails the risk of imposition of administrative sanctions under Article 17.14 of the Code of Administrative Offenses (a fine totalling one half of the amount to be recovered from the debtor, but no more than one million roubles).

The Bank of Russia may also revoke the credit institution's license if the bank is found more than once during the course of the year to be failing to comply with requirements covered in execution orders of courts of law or arbitrazh courts to recover funds from accounts (deposits) of customers of this credit institution (on condition that funds are available in accounts (deposits) of these customers).

If the bank debits funds in compliance with execution orders while transactions involving such funds are found to be suspicious, the bank will face an increase in the volume of suspicious transactions by its customers, which may affect the assessment of the bank's financial position in accordance with Bank of Russia Directive No. 4336-U[1]. This may also entail the risk of the bank's internal control measures being recognized to be in breach of laws and regulations of the Bank of Russia due to a high risk (uncontrolled by the bank) of the bank's services getting abused for ML/TF purposes. Accordingly, the bank faces the risk of sanctions under Article 74 of the Law *On the Central Bank*[2] — a prescriptive order, penalties all the way to license revocation.

Taking into account the existing practices, banks look for ways out and solutions to the problem on their own, on a case-by-case basis, bearing in mind every aspect of the context, the volumes of transactions in question, the available resources and the bank's attitude toward this problem. A list of the most common solutions used by each bank individually follows:

1. The majority of banks pursue the official position of the Bank of Russia covered in Guidance Notes 4-MR, according to which banks must process payments under execution orders and take necessary steps outlined in the Guidance Notes. I believe this position to be correct. However, it is more suitable for small and medium banks where the volume of payments under execution orders is extremely negligible, since the bank may face a serious problem in case of substantial volumes of suspicious transactions related to execution orders, as described above.

2. This problem is solved by getting the bank's security service involved. Its approaches are not always clear for the compliance team, but are very effective nonetheless. It is a good and effective option. However, it requires having a robust security service with extensive contacts and capabilities, which only a few credit institutions can afford, unfortunately.

[1] Bank of Russia Directive No. 4336-U of April 3, 2017 On Assessment of the Financial Position of Banks (together with the Methods of Assessment of the Transparency Indicators of the Bank's Ownership Structure).

[2] Federal Law No. 86-FZ of July 10, 2002 On the Central Bank of the Russian Federation (Bank of Russia).

3. An authorized bank employee or staff of the financial monitoring departments can use personal ties with colleagues from other banks and give them advance warning about funds credited to their customers' accounts with the use of suspicious execution orders. In this case, even though a payment gets "released" by one bank, it will end up getting frozen by another bank. I believe this to be a very effective method that will potentially put an end to suspicious schemes with the use of execution orders, as it will eliminate the opportunity to spend funds obtained with the use of a scheme involving executive proceedings. However, employees of one bank need to have extensive contacts with employees of other banks in order to implement this mechanism. Also, this method fails to solve the problem in cases when the funds are sent to court enforcement officers to be subsequently forwarded to the intended individual beneficiaries.

4. Ban on crediting funds to the account. This method eliminates the need to choose between a violation of AML/CFT legislation and a violation of laws on executive proceedings. Yet this method is difficult to implement from the legal perspective.

Since June 1, 2018, Article 858 of the Civil Code of the Russian Federation allows supplementing the bank account agreement with a clause that mentions cases in which the bank is obliged to refuse to credit funds to the customer's account, unless the law provides otherwise.

Even though multiple publications after adoption of this provision stated that its purpose was to enhance the bank's possible response to AML/CFT risks (including possible refusal by the bank to credit funds in case of suspicions that transactions are executed for ML/TF purposes), the relevant amendments have not been made to Law No. 115-FZ to this day.

The right of a credit institution to refuse to process a transaction due to the imperative legislative provision does not apply to the crediting of funds transferred to a customer's account.

Accordingly, the bank is obliged to credit the funds to the customer's bank account and, when the relevant grounds exist under Law No. 115-FZ, decline to process the customer's payment instructions to debit the funds from the account.

5. Establishment of strict criteria for opening an account. In most cases, schemes are used by shell companies that are opened for purposes of carrying out suspicious transactions, including those under execution orders. Most commonly, a company registered a few months ago opens a business account and presents an execution order to the bank, under which the company is obliged to pay salary arrears to its employee in an amount that far exceeds the average-market salaries for the given occupation, region, etc.

Strict criteria for the customer opening an account will undoubtedly help to avoid future problems in serving this customer. Yet this approach is suitable for small banks main revenue of which is generated from business areas other than cash and payment processing services.

Thus, "weak points" in Russian legislation used by shadow companies in their criminal schemes and the lack of a systemic mechanism for combating such schemes at the legislative level encourages banks and the overall banking industry to improve their internal control measures, enhance the efficiency of information sharing, and take preventive steps with the support of the Bank of Russia and Rosfinmonitoring.

Further development of mechanisms for combating suspicious schemes with the use of execution orders with the support of the Bank of Russia and Rosfinmonitoring will result in a substantial reduction in the volume of such suspicious transactions in the near future, while in some cases their execution will be completely impossible. This problem is as old as time itself. The Bank of Russia and Rosfinmonitoring have been working to address it for a long time, and this issue has been discussed by bank associations on multiple occasions. The effective methods currently in use have already caused the decrease in the volume of such transactions, and there is strong confidence that an effective legislative mechanism for combating this scheme will be developed in the immediate future, bringing such volumes to nil.

NEW TECHNOLOGIES

DIGITAL IDENTITY: THE FATF VIEW

In March 2020, the FATF released the Guidance on Digital Identity. This topic has attracted the interest of the FATF primarily due to the growing volume of digital financial transactions and the understanding of how customer due diligence measures are used in the processing of digital financial transactions

Inessa Lisina,
Deputy Editor-in-Chief

Today's world is unimaginable without online services for delivery of goods and services to the general public, and the volume of such transactions is expected to rise in the future. This trend is becoming more and more discernible in the context of the existing restrictions due to the ongoing global pandemic. The growing number of online transactions requires all operators of the financial infrastructure to gain a more in-depth understanding of how individuals are identified in digital identity (ID) systems. This is an important aspect of customer due diligence measures implementation in accordance with FATF Recommendation 10, which sets out a number of mandatory customer due diligence requirements for reporting entities and regulated organizations. However, many of them face the question: How does one verify the identity during remote interaction with the customer, i.e. via email or by phone? This Guidance is devoted to explaining these and other related issues. Notably, the authors place great emphasis on the fact that the document describes only processes of identification of physical persons.

The Guidance consists of several chapters, including FATF customer due diligence requirements, benefits and risks of using digital ID systems, assessment of the digital ID systems reliability under risk-based approach (RBA) to customer due diligence, digital ID examples and national practices, a description of a basic digital identity system and its participants, identification principles for sustainable development, etc.

The transition to digital identity systems has given rise to multiple issues and changes in the process of interaction with customers. Identity verification was traditionally based on "manual controls": employees of regulated organizations compared photos in personal identity documents with the appearance of the customer applying for a service. With this method, the risk of error was quite high, as methods of authentication of presented identity documents were not employed.

Verification process used in Digital ID systems is based on various biometric technologies, uses online resources, mobile phone interface (built-in cameras, microphones, and other elements), digital device identifiers (e.g., IP addresses, mobile phone numbers, global position system (GPS) geolocation, etc.) As part of digital identity systems, digital technologies can be used in various ways, including to search for information in electronic databases in order to verify digital credentials and biometrics, to use the infrastructure of digital application program interfaces, platforms, protocols, etc.

The Guidance states that there are at least three types of factors that can be used to authenticate someone: ownership factors (e.g., cryptographic keys), knowledge factors (e.g., a password), and inherent factors (e.g., biometrics).

All of these data are meant to facilitate online identification/verification and authentication of an individual. Moreover, such systems use mechanism of authentication of identity documents presented. Therefore, they are more accurate, safe, more confidential, and convenient for identification/verification of individuals in all sorts of situations, e.g. when opening an account, at "on-boarding", or in the course of performing transactions, as well as during ongoing monitoring of financial transactions.

The FATF Guidance also examines the application of Recommendation 17 (Reliance on third parties). According to its provisions, member states may permit regulated entities to rely on third parties to apply customer due diligence measures, which also includes identification/verification of customers. The digitalization of financial services sector has increased the importance of reliable, independent digital ID systems for purposes of financial inclusion, especially in developing countries.

It is important to remember that if digital identity systems do not cover the entire population or its majority, they may cause financial exclusion of specific groups of the population, which poses ML/TF risk. Jurisdictions must take all the available measures and steps to prevent a situation like this.

Digital identity is also important in the context of implementation of Recommendation 11 (Record

Keeping) by member states. It obligates financial institutions to store all records obtained as a result of customer due diligence, including copies of identity documents. Such data should be available to the relevant authorities. These issues may also arise in the context of using digital identity systems.

Speaking of digital identity, one must remember about a number of cyberthreats that any digital system can be exposed to. The Guidance describes the following types of possible threat sources:

- cyberattacks and security breaches leading to the leakage of personal information and its misuse by impostors
- violations committed by ID Service Providers.

When personal data are stolen, this may result in impersonation. In this situation, an impostor poses as the genuine owner of stolen identity data or uses stolen documents, including photo or data substitution in them. Criminals may also develop "synthetic identities" by combining real (usually stolen) and fake information to create new (synthetic) identity information. Unlike impersonation, a criminal pretends to be someone who does not exist in the real world instead of posing as a real person.

Another major problem concerns theft of authentication credentials such as logins, passwords, secret codes, or other information that can be used to access services, personal data, and other digital services. Modern reliable digital identity systems should be ready for such challenges and develop mechanisms to combat them. One of the solutions is multi-factor authentication (e.g., with the help of SMS codes).

Another possible solution is authentication based on biophysical elements: fingerprints, iris scans, facial recognition. The use of such methods is currently becoming more and more widespread, as biometric data can be currently recognized using smartphones or other digital devices. However, biometric characteristics could be stolen in bulk even though these types of attacks are difficult to accomplish.

Obviously, digital ID systems collect and process a vast array of personal data. For this reason, digital identity systems must guarantee data protection and privacy (hereinafter DPP). These requirements should apply to Digital ID Service Providers. Therefore, in accordance with FATF Recommendation 2, AML/CFT and DPP authorities should seek to cooperate to ensure compatibility of the relevant requirements and rules.

An important issue addressed in the Guidance is a digital ID system for refugees or asylum seekers. The problem of their identification is unique in many ways. As of the end of 2018, the office of the United Nations High Commissioner for Refugees (UNHCR) estimated there were 25.9 million refugees and 3.5 million asylum seekers globally.

Host countries and a number of internationally recognized authorities are responsible for issuing proof of official identity to refugees. Many refugees often do not possess identity credentials while others may never have been issued with official identity cards or other credentials due to discrimination or for other reasons. In order to avoid harming refugees or asylum seekers, the host countries cannot appeal to their country of origin in order to verify their identity without a person's consent, as they may be at risk of harm. Therefore, according to international standards, in the course of identity proofing of refugees one should rely more on evidence obtained during in person applications and interviews.

The UNHCR developed a digital ID system to bring migration flows under control. By March 2020, over 9 million refugees in 72 countries had been biometrically enrolled in the system. Both asylum seekers' and refugees' identity credentials vary according to host country requirements, but contain facial image, biographic information and other elements that uniquely identify a person. The identity credentials also have a printed bar code or QR code and a unique reference number of the holder.

The importance of digital identity issues has been now recognized at the global level. As a result, these issues are reflected both in the Principles on Identification for Sustainable Development and in the ID2020 project supported by the UN as part of the 2030 Agenda for Sustainable Development Goals. The project involves creating a prototype of a digital ID system, and the plan is to provide all people on the planet with digital IDs by 2030. The system will be based on the blockchain technology (i.e., encrypted data in a distributed database), which will combine the existing record keeping systems pertaining to personal IDs and enable users to access their personal data from any global location. An experimental version of the platform is scheduled for completion by the end of 2020.

These measures will become a major step forward in the development of the personal identification and verification system in the digital world. In its turn, the FATF's experience summarized in the Guidance will contribute to the understanding of digital identity, primarily for AML/CFT purposes in the context of digital financial services.

E-MONEY

MEASURES TO MITIGATE ML/TF RISKS IN THE CONTEXT OF CRYPTOCURRENCY TRANSACTIONS PROVIDED BY LEGISLATIVE ACTS OF THE EUROPEAN UNION AND EU MEMBER STATES

Vladimir Glotov,

Deputy Director of the Federal Financial Monitoring Service, Candidate of Economics, Professor, Director of the Institute of Financial Technologies and Economic Security (IFTES) of the National Research Nuclear University MEPhI (Moscow Engineering Physics Institute)

Igoris Krzhechkovskis,

Senior Instructor at the Basic Department of Financial and Economic Security at Plekhanov Russian University of Economics

In exploring international crime trends and changes in "strategic priorities" of cross-border criminal organizations, it is worth noting that crimes targeting the financial system have always been and remain one of the most profitable criminal endeavors. A particular cause for concern is the growing interest of criminals in not just targeting the relatively vulnerable banking and financial institutions but also in rapidly developing their skill set that enables them to effectively use advanced computer technologies, including products of the rapidly growing crypto asset or cryptocurrency market, to both commit crimes and launder illicit proceeds.

It should be noted that the emergence of bitcoin in the not so distant past as the first representative of this market immediately caused concern and a negative reaction from not just AML/CFT experts but also law enforcement specialists involved in fighting fraud and crimes in the sphere of computer technologies. This negative reaction was provoked by just one factor that also happens to be the chief advantage of bitcoin: the ability to make purchases and carry out transactions, including cross-border transactions, anonymously and exchange bitcoin into cash in a relatively simple way.

Unfortunately, international institutions tasked with AML/CFT efforts and supervision of the banking and financial sector were extremely late in coming up with the appropriate countermeasures. This enabled the cryptocurrency market to grow actively, which in turn resulted in rapid multiplication of bitcoin-like crypto assets as well as in colossal growth in the value of the assets themselves, which brought about something like a gold rush with all the associated negative consequences in the form of bankruptcies of unfortunate investors, purchases of fake crypto assets, large scale embezzlement on cryptocurrency exchanges, and so forth. For this reason, the need for both stringent regulation of this market and its integration into the global AML/CFT system compelled the relevant international organizations to take a number of steps toward mitigating risks and threats associated with bitcoin and similar "tools".

The relevant EU institutions have been long since actively analyzing the potential risks and vulnerabilities of using cryptocurrency transactions for payments in various illicit schemes as well as for laundering illegally obtained property and money.

This issue was for the first time highlighted as part of the Supranational ML and TF Risk Assessment (SNRA) conducted by European Commission experts in pursuance of Directive 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (Fourth EU AML/CFT Directive). Although at the time of SNRA entities conducting cryptocurrency transactions did not appear on the list of entities subject to primary financial monitoring either in legislative acts of the European Union or in FATF Recommendations, representatives of law enforcement agencies and private financial companies were already aware of instances of bitcoin and other cryptocurrencies being used to pay for drugs or conceal illicit proceeds.

AML/CFT experts were well aware of all vulnerabilities that were effectively used by the unregulated and

virtually uncontrollable yet actively expanding cryptocurrency market: anonymity and major difficulties for tracking down and identifying individuals performing the transactions, real-time exchange and transfers of funds in cryptocurrencies across national borders, a significant shortage of knowledge and capabilities of law enforcement agencies needed to determine the actual location of cryptocurrencies in order to seize them.

In light of the pressing nature of the problems in question, in drafting the First Report of the European Commission addressed to the European Parliament and the Council on the assessment of risk of money laundering (ML) and terrorist financing (TF) affecting the internal market and relating to cross-border activities with a view to determining the conditions under which suppliers/merchants of ML/TF services are used, which was approved on June 26, 2017 (hereinafter "the First SNRA Report[1]), the experts involved in the development of this document did their best to analyze both risks and vulnerabilities of cryptocurrencies in as much detail as possible.

The problems of the crypto market in the context of cryptocurrency use for ML/TF purposes were analyzed as part of the first SNRA based on statistical data available at the end of 2015. According to data at the disposal of the assessors, the cryptocurrency market had a capitalization of seven billion euros at the time. It was noted that a substantial segment of that market – miners,

[1] https://publications.europa.eu/en/publication-detail/-/publication/ce3cb15d-5a5a-11e7-954d-01aa75ed71a1.

entities offering services involving the opening and administration of cryptocurrency wallets, exchanges, and users themselves – were located outside EU member states. It was also concluded that this market was growing at a very rapid pace. According to data presented in the First Report, in the space of just one year (based on a comparison of data for the last three months of 2014 and 2015) the number of cryptocurrency wallets increased from 7.4 million to 13 million globally. During the same period there was a notable increase in the number of commercial entities that accepted bitcoin as a legal tender: from 80 to 110 thousand.

In assessing the risk of ML/TF threats and vulnerabilities of the cryptocurrency market, European Commission experts analyzed information about potential cryptocurrency uses in the criminal world. The level of ML/TF threats was determined to be fairly low. The primary arguments to support this conclusion were as follows:

- although the number of reports about potential use of cryptocurrency for TF purposes increased and cases were reported of members of terrorist groups exchanging cryptocurrency usage instructions, at the time of the First Report preparation criminals needed to possess a sufficient level of knowledge as well as be able to use additional technologies, which – despite the obvious advantages of bitcoin – reduced its value for terrorists;
- the number of ML criminal cases containing facts of cryptocurrency use was negligible. Just like in the case of TF analysis, it was observed that cryptocurrency transactions required additional resources, unlike, for example, electronic money transactions. Also, law enforcement agencies did not possess information that would indicate that the amounts of funds that could be laundered using cryptocurrencies were substantial.

When the assessors presented their report on the vulnerabilities of the AML/CFT system coming from the cryptocurrency market, the situation turned out to be completely different. A considerable level of vulnerability was detected in terms of both TF and ML. The main reasons were:

- the lack of legal regulation and control over the cryptocurrency market in the European Union as well as the lack of requirements for this market participants to apply AML/CFT norms;
- anonymity of transactions and lack of obstacles whatsoever to transfers of funds without proper identification of their owner;
- unobstructed and virtually instantaneous cross-border transfers of cryptocurrency to any location on the planet with the use of Internet resources and information technologies potential;
- the non-existence of a centralized cryptocurrency transfer system;
- fairly low capabilities of financial intelligence units (FIUs) and law enforcement agencies to monitor transactions made with the use of cryptocurrency wallets or to block suspicious transactions and deals in this sector without delay, as well as to pursue effective international cooperation.

As a key measure to mitigate the vulnerability detected, the European Commission was advised to immediately draft and present for consideration amendments to AML/CFT legislation, based on which cryptocurrency exchanges and entities providing cryptocurrency wallet opening and administration services would be put on the list of entities subject to primary financial monitoring and would be obligated to apply all the relevant AML/CFT measures. Complying with this requirement and implementing the entire range of measures aimed at mitigating other threats and vulnerabilities, **on May 30, 2018 the European Parliament and the Council of Europe approved Directive 2018/843 on Anti-Money Laundering and Combating the Financing of Terrorism (so-called Fifth EU AML/CFT Directive)[2].**

[2] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015L0849.

The provisions of the Fifth Directive are primarily aimed at:

- limiting anonymity that was ensured by the use of cryptocurrencies, enhancing control over the activities of entities providing cryptocurrency wallet opening and administration services, as well as enhancing control over transactions performed using so-called prepaid cards;
- enhancing the transparency of economic
- and financial activities by developing registers of ultimate beneficial owners of companies, trusts and other legal entities;
- expanding the list of criteria for assessment and designation of high-risk countries, as well as improving the rules of safety/risk mitigation associated
- with cross-border financial transactions;
- establishing requirements for EU member states regarding the creation of a central
- database of registers of accounts or specialized systems designed for finding information about opening of accounts;
- improving collaboration among institutions overseeing compliance with AML/CFT measures, including information exchange among them.

In drafting this document, the experts devoted particular attention to the problem of control over virtual currency transactions. It was observed that the European financial system could face major security problems in the face of the use of virtual currencies. AML/CFT stakeholder institutions should obtain effective tools for monitoring and controlling virtual currency transactions. FIUs should have access to information that makes it possible to link a cryptocurrency to the identity of its owner. Although virtual currencies are often used as a means of payment, they can also be used for other purposes such as exchange and investment.

The goal of the Fifth Directive is to put in place a system of control over all transactions with the use of cryptocurrencies.

Pursuant to the requirements of the Fifth Directive, entities providing cryptocurrency conversion services and wallet administrators have been added to the list of entities subject to primary financial monitoring. It has been established that an administrator of a cryptocurrency wallet is an entity providing services designed to ensure the safety of private encryption keys as well as administration, storage, and transfer of cryptocurrencies on behalf of customers. At the same time, EU member states should develop and implement a system for registering the providers of such services.

Once these requirements have been integrated into national laws, all entities providing such services will be obligated to apply AML/CFT measures indicated both in EU legislative acts and in the FATF requirements on which the Fourth EU Directive is based.

The text of the Fifth Directive, based on which EU member states should develop and implement the relevant internal regulatory acts by January 10, 2020, also includes a definition of a virtual currency. It is defined as “a digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded electronically”.

In order to develop additional measures of control over cryptocurrency transactions, experts of the European Commission conducted further analysis of virtual currency threats and vulnerabilities as part of the Second AML/CFT SNRA (the report was approved on July 24, 2019[3]). The conclusions of this report state that ML/TF risks for the financial system of the EU are substantial when it comes to the use of cryptocurrencies. The report also notes that the definition of virtual assets and entities

[3] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017SC0241.

providing virtual asset services contained in the FATF documents is broader than that in the Fifth EU AML/CFT Directive.

Compared to the findings of the first SNRA Report, there is a notable increase in the level of threats posed by cryptocurrency transactions for the AML/CFT system. It has been found that law enforcement agencies possess information about large sums of illicit assets getting exchanged into cryptocurrencies; services involving virtual currency exchange and cross-border transfers are provided to users without any registration; alongside bitcoin, other kinds of virtual currencies have entered the market and are rapidly gaining popularity. Law enforcement agencies are particularly concerned about the possibility to conduct a quick initial cryptocurrency offering (ICO) as well as carry out cryptocurrency exchange transactions in countries where the payer and the payee are not present physically at the time of transaction.

The assessment findings show that cryptocurrency transactions are used by terrorist groups. There has also been an increase in the number of investigations of other crimes committed with the use of electronic money. It has been found that cryptocurrency transactions are used by a wide range of international organized crime, with cybercriminals and drug dealers identified as the most active users.

The rating of vulnerability to the risks of cryptocurrency transactions remains at a high level as before. According to the findings of assessors, activities of providers of all kinds of cryptocurrency-related services are not subject to full control of EU legislative acts, hence the recommendation was issued to harmonize EU AML/CFT requirements with the FATF Recommendations. Although new EU regulatory acts have partly solved this problem, their application began only recently. Meanwhile, cryptocurrency transactions can be carried out using easily accessible technologies that ensure anonymity (the Internet, international money transfers, special technological tools). One of the available examples of the implementation of EU requirements in terms of AML/CFT measures aimed at controlling the cryptocurrency market is the experience of the Republic of Lithuania, where the relevant amendments to national AML/CFT legislation were approved by Parliament (Sejm of the Republic of Lithuania) on December 3, 2019 in the form of amendments to the Anti-Money Laundering and Combating the Financing of Terrorism Law (hereinafter the "AML/CFT Law")[4]. According to these amendments, the text of Article 2 of the AML/CFT Law "**Basic Concepts of this Law**" was supplemented with the following definitions:

Virtual currency deposit wallet — virtual currency addresses generated using a public key and designed to store and administer virtual currencies that have been entrusted to other individuals or legal entities (third parties) but remain under the ownership of the respective clients.

Operator of virtual currency deposit wallets — a legal entity registered in the Republic of Lithuania or a branch of a legal entity based in an EU member state or a foreign country and registered in the Republic of Lithuania, which provides virtual currency deposit wallet administration services on behalf of clients.

The following entities were added to the list of other (non-financial) entities subject to primary financial monitoring:

- operators of virtual currency exchanges;
- operators of virtual currency deposit wallets.

Initial cryptocurrency offering (ICO) — an offer made by a legal entity registered in the Republic of Lithuania or a branch of a legal entity based in an EU member state or a foreign country and registered in the Republic of Lithuania, either directly or through an intermediary, to purchase its virtual currency with money or another virtual currency for purposes of raising capital or investments.

Public key — a code consisting of letters, numerals and/or symbols intended for client identification and generation of the client's virtual currency address.

[4] https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/9564d1a21a5b11eaa4a5fa76770768ee?positionInSearchResults=1&searchModelUUID=542ac2c7-5a9a-4cf3-ba25-100b7df58b94.

Virtual currency — a means of payment that has a digital value but does not have legal status as a currency or money, which is not issued or guaranteed by a central bank or another state institution, and which is not necessarily linked to a currency, but which is recognized by individuals or legal entities as a means of exchange and which can be transferred, stored, or sold by electronic means.

Virtual currency address — an address (account) generated using a public key in the blockchain, consisting of letters, numerals, and/or symbols, based on which the blockchain attributes a virtual currency to its owner or recipient.

Operator of a virtual currency exchange — a legal entity registered in the Republic of Lithuania or a branch of a legal entity based in an EU member state or a foreign country and registered in the Republic of Lithuania, which provides for a fee virtual currency exchange, purchase and/or sale services.

Lithuanian FIU was charged with function of the primary supervisory authority for these entities. Based on amendments made to **Part 9 of Article 4 of the AML/CFT Law "Obligations of Institutions Responsible for Anti-Money Laundering and Combating the Financing of Terrorism",** it is now stipulated that directives and rules governing the implementation of AML/CFT measures intended for operators of virtual currency exchanges and virtual currency wallet operators shall be approved by the Financial Crimes Investigation Service at the Ministry of Internal Affairs of the Republic of Lithuania (Lithuanian FIU) following their approval by the Lithuanian Bank and the Ministry of Finance of the Republic of Lithuania.

In order to grant the FIU access to information about virtual currency transactions, pursuant to **amendments to Clause 1 of Article 7 "Rights of the Financial Crimes Investigation Service in the Course of Implementation of AML/CFT Measures"**, Lithuanian FIU has been authorized to receive documents and information about monetary or cryptocurrency transactions and deals as well as other information needed to perform functions and accomplish tasks outlined in this Law not just from all institutions responsible for AML/CFT, other government agencies, financial institutions, other **entities subject to primary financial monitoring** but also from entities making an initial cryptocurrency offering (ICO).

In accordance with additions made to Part 1 of Article 9 "Identification of the Client and the Beneficiary", entities subject to primary financial monitoring are obligated, just like in other cases, to determine and verify the identity of the client and the beneficiary prior to processing a virtual currency exchange transactions or deals using virtual currencies whose amount equals to or exceeds 1,000 euros, or the corresponding amount in a foreign or virtual currency, either before depositing funds to a virtual currency deposit wallet or before debiting funds from this wallet.

For purposes of identifying cases in which several interconnected virtual currency transactions are made, **Part 11 of Article 9** was supplemented, according to which several virtual currency transactions should be considered as interconnected if the client:

- performs several virtual currency exchange transactions or several virtual currency transactions in the space of 24 hours and their amount is equal to or exceeds 1,000 euros or the corresponding amount in a foreign currency or virtual currency, or performs several transactions to deposit or debit virtual currency from a virtual currency deposit account in the space of 24 hours and their amount is equal to or exceeds 1,000 euros or the corresponding amount

- in a foreign currency or virtual currency; performs several transactions in the space of 24 hours involving the purchase of virtual currency from an entity making an initial cryptocurrency offering (ICO) and their amount is equal to or exceeds 3,000 euros or the corresponding amount in virtual currency.

The act also defines measures aimed at storage of information by entities subject to primary financial monitoring - operators of the virtual currency market. According to additions made to Article **19 "Storage of Information" of the AML/CFT Law of the Republic of Lithuania,** operators of virtual currency exchanges and virtual currency deposit wallet operators are obligated to maintain a special book for registering monetary transactions performed by clients as well as store information that makes it possible to link the virtual currency address to the identity of the virtual currency owner for up to 8 years from the date when transactions were completed or the business relationship with the client ended.

According to additions made to Article **20 "Disclosure of Information to the Financial Crimes Investigation Service"** of the AML/CFT Law, operators of virtual currency exchanges must disclose to the Financial Crimes Investigation Service the information proving the identity of the customer and information about virtual currency exchange transactions completed or virtual currency deals made if the amount of this transaction or deal is equal to or exceeds 15,000 euros or the corresponding amount in a foreign currency or virtual currency. It does not matter whether the deal has been effected through one or several interconnected transactions. Interconnected monetary transactions are foreign currency exchange transactions or foreign currency deals completed in the space of 24 hours when their amount is equal to or exceeds 15,000 euros or the corresponding amount in a foreign currency or virtual currency.

In order to implement the requirements regarding the registration of entities providing virtual currency exchange services and virtual currency deposit wallet administration services, additions were made to the text of **Article 25 "Requirements for Legal Entities and Individuals Associated with Entities Providing the Services of Trusts or Corporate Services as well as Real Estate Agents,** according to which a legal entity that has commenced or discontinued operations as a virtual currency exchange operator or a virtual currency deposit wallet administrator shall – within 5 business days of commencement or cessation of such operations – notify the administrator of the register of legal entities about commencement or cessation of operations as a virtual currency exchange operator or a virtual currency deposit wallet administrator. In presenting such information, the virtual currency exchange operator or the virtual currency deposit wallet administrator confirms that he personally or members of his governing or supervisory bodies and beneficiaries are familiar with legislative acts on AML/CFT and their relevant requirements.

AML/CFT requirements for entities making an initial cryptocurrency offering (ICO) were incorporated into the new **Article 25 of the AML/CFT Law "Requirements for Entities Making an Initial Cryptocurrency Offering (ICO)".** Based on these requirements, such entities shall:

- establish and verify the identity of the person buying virtual currency, and the person's beneficiary, by following the procedure established by the AML/CFT Law, prior to processing one-time or several interconnected monetary transactions or foreign currency transactions or entering into a deal whose amount is equal to or exceeds 3,000 euros or the corresponding amount in a virtual currency (the value of the virtual currency is determined

- at the time of the transaction or deal); in this case it does not matter whether the deal has been effected through one or several interconnected transactions; all appropriate measures to determine the source of assets or funds involved in the business relationship or transaction should be applied;

- as and when requested by the Investigation Service, present the information requested within 7 business days of receipt of the request.

If the request of the Service for disclosure of information reasonably states a shorter timeframe for disclosure of information, the entities making the initial cryptocurrency offering (ICO) must present the information requested within the timeframe specified in the request;

- store – for 8 years from the date of completion of the transaction with the person who bought virtual currency – copies of personal identity documents specified in Part 2 of this article, details of the beneficiary's personality, records of direct video transmission , other data received during the course of identification of the person buying virtual currency, documents of accounts and/or contracts (original documents) and data and documents proving the monetary transaction, virtual currency transaction or deal, as well as other legally binding documents and data relating to monetary transactions, virtual currency transactions, or deals.

Entities making an initial cryptocurrency offering (ICO) or their employees are prohibited from notifying the client or other parties that the information about monetary transactions or deals made by the client or any other information has been disclosed to the Financial Crimes Investigation Service or other supervisory authorities.

In light of the foregoing, it should be noted that the above-mentioned experience of the European Union in developing and enacting AML/CFT related legislative acts is important first of all because these standards are binding on all EU member states and must be implemented within the timeframes approved through a consensus reached both at the level of the European Council (which hosts high-ranking representatives of all EU member states) and the European Parliament whose members were elected by citizens of EU member states. Therefore, by following the example of the Republic of Lithuania, measures to prevent the use of crypto assets for ML/TF purposes should be approved in legislative acts of EU member states by January 10, 2020, as prescribed by the Fifth EU AML/CFT Directive.

As already mentioned, the relevant preventive legislation of the Republic of Lithuania was developed using not just standards of the European Commission but also the FATF Recommendations as well as the experience of countries that are not EU member states, which has made it possible to create a more comprehensive system for combating the use of cryptocurrencies for criminal purposes.

A review of the experience of developing new mechanisms of the AML/CFT system covered in this article prompts the conclusion that only by using an integrated approach to detection of problems involving the use of cryptocurrencies in money laundering and other crimes, by exploring this problem in detail, implementing measures aimed at national assessment of risks and threats, drafting and enacting new international acts of legislation designed to combat money laundering and terrorist financing, as well as strictly complying with their provisions at the national level, we will be able to conclude that these new challenges to the global financial system are being effectively countered. Notably, such international organizations as the FATF and FATF-style regional bodies, as well as the European Commission, UNODC, Interpol, and others should actively cooperate with partners and continuously implement measures aimed an in-depth study of this phenomenon and take steps within their respective scope of authority to monitor compliance with international legislative requirements at the national level. The results of such monitoring, which can help detect and neutralize potential "safe havens" in specific countries and jurisdictions as well as in the cyberspace, will significantly complicate the use of crypto assets by organized crime in their illegal undertakings. Yet this task will have to be accomplished in challenging conditions considering the fact that crypto assets are being used increasingly more actively and extensively and are being integrated into the system of legitimate economic relations, with each passing day becoming more accessible to common citizens in their day-to-day activities.

References:

1. International standards on combating money laundering and the financing of terrorism & proliferation – FATF Recommendations (updated June 2019) [E-resource] Accessible at: https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf (Date 25.12.2019)

2. Directive 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing [E-resource]. Accessible at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015L0849 (Date 25.12.2019)

3. Report from the Commission to the European Parliament and the Council on the assessment of the risks of money laundering and terrorist financing affecting the internal market and relating to cross-border activities. COM/2017/0340 final [E-resource] Accessible at: https://publications.europa.eu/en/publication-detail/-/publication/ce3cb15d-5a5a-11e7-954d-01aa75ed71a1 (Date 25.12.2019)

4. Report from the Commission to the European Parliament and the Council on the assessment of the risks of money laundering and terrorist financing affecting the internal market and relating to cross-border activities (SWD (2019) 650 final) [E-resource] Accessible at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017SC0241 (Date 25.12.2019)

5. European Commission Staff Working Paper 2/2 accompanying Report from the Commission to the European Parliament and the Council on the assessment of the risks of money laundering and terrorist financing affecting the internal market and relating to cross-border activities (COM(2019)370 final) Accessible at: file:///C:/Users/Expert/Desktop/HLA2021/Reports2019/Monthes/September/SNRAeuII/WorkingPaperSNRAII2019.pdf (Date 25.12.2019)

6. Directive 2018/843 of the European Parliament and of the Council of 30 May 2018 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing [E-resource]. Accessible at: https://eur-lex.europa.eu/legal-content/EN/XT/?uri=CELEX%3A32018L0843 (Date 25.12.2019)

7. Law on Amendments to the Law of the Republic of Lithuania on Combating Money Laundering and the Financing of Terrorism No. XIII-2584, adopted by the Parliament (Sejm) of the Republic of Lithuania 3/12/2019 [E-resource] Accessible at: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/9564d1a21a5b11eaa4a5fa76770768ee?positionInSearchResults=1&searchModelUUID=542ac2c7-5a9a-4cf3-ba25-100b7df58b94 (Date 25.12.2019)

8. Kucherov I. Cryptocurrency: (ideas of alternative payment means legal identification and legitimation): monograph. – M.: JurInfoR Center, 2018.

AML/CFT EDUCATION AND SCIENCE

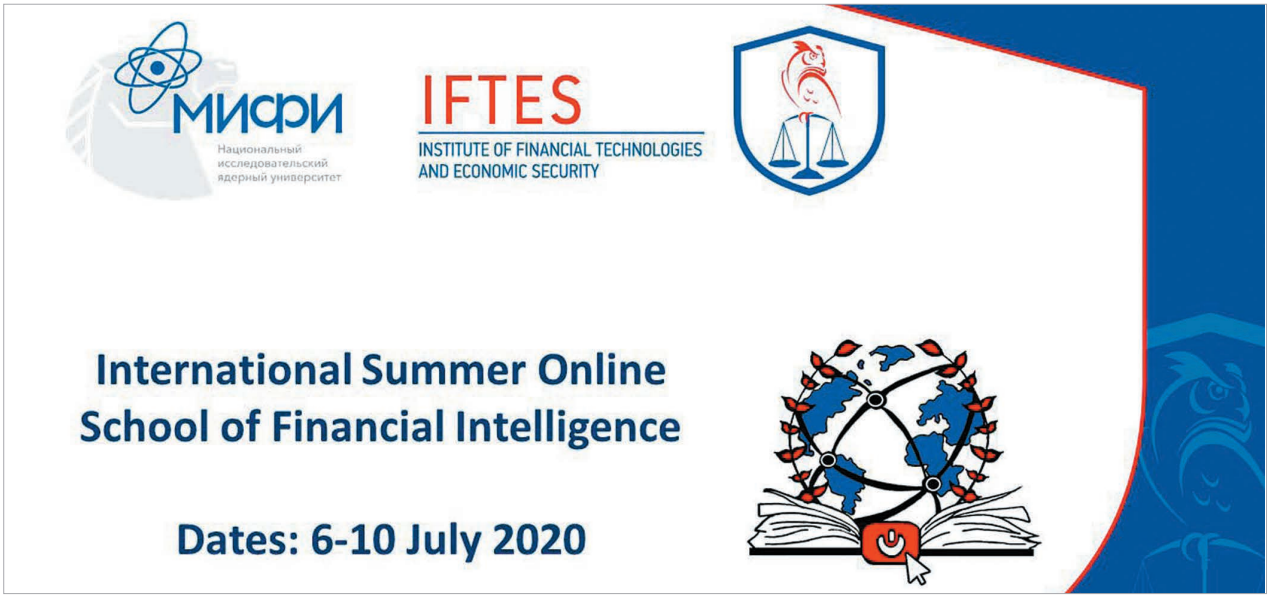
INTERNATIONAL SUMMER ONLINE SCHOOL OF FINANCIAL INTELLIGENCE TOOK PLACE

On July 6-10, the Institute of Financial Technologies and Economic Security (IFTES) NRNU MEPhI (the International Network AML/CFT Institute's participating university) held International Summer Online School of Financial Intelligence in English

School's work was focused on the main AML/CFT/CPF definitions, concepts and related key issues.

The working language of the whole event was English, which made it possible to attract the attention of participants from 15 countries and 10 universities.

At the School opening, Nikolai Morozov, the co-head of the School, Ph.D. in Law, Associate Professor of the Financial Monitoring Department No. 75, Head of the International Cooperation Department of the Institute of Physics and Technology of Economics (IFTES), NRNU MEPhI addressed the audience with a welcoming speech.



The main lectures were delivered by Igoris Krzhechkovskis (Lithuania), an international AML/CFT/CPF expert, Associate Professor of the Financial Monitoring Department No. 75 of the Institute of Financial Technologies and Economic Security (IFTES), NRNU MEPhI.

Core lecture topics were:

- What is AML/CFT system and financial intelligence?
- International AML/CFT System (key players and best practices)
- AML/CFT areas: private and public sectors
- New IT technologies in financial intelligence
- The ultimate phase of AML/CFT efforts- criminal investigation, arrests, confiscations.

Nadezhda Kuznetsova, Viktor Sushkov, Egor Malakhov and Soumujit Mukherjee (India) acted as tutors in the practical classes.

During the practical exercises, the following topics were used:

- What skills are needed to work in financial intelligence?
- What is the strength of financial intelligence? The world without illusions!
- Beware: shell companies facilitate ML/TF
- The world of financial crimes: behind the scenes, on the "ground".

The work in the practical classes was active and interesting. Participants from different countries were able not only to solve practical cases suggested by the tutors, but also to share their experience in combating money laundering.

During the final discussion, the participants' assignment outcomes were discussed.

The School was attended by over 50 participants from Russia, Belarus, Kazakhstan, Uzbekistan, India, Zambia, Indonesia, Bangladesh, Mexico, Algeria, Iraq, the Czech Republic and Morocco.

38 participants who successfully passed the final tests received certificates.

It is planned to conduct such an event annually.

https://mephi.ru/

INNOVATIVE APPROACHES IN THE EDUCATIONAL PROCESS AND IMPROVEMENT OF THE PERSONNEL TRAINING SYSTEM IN THE AML/CFT AREA

Representatives of International Network AML/CFT Institute and ITMCFM experts took part in international scientific and practical conference named "Enhancement of law enforcement educational capacity: modern challenges and solutions"

The conference hosted by **the member of the International Network AML/CFT Institute – the Academy of the General Prosecutor's Office of the Republic of Uzbekistan** was held online via video conferencing. The conference coincided with the special event – the second anniversary of the Academy.

The conference agenda included the Plenary meeting as well as break-out sessions dedicated to the following topics: "Methods of arranging the educational process in the contemporary context"; "Role and contribution of legal science and education to fight against corruption"; and "Improvement of investigative skills: cross-cutting issues and ML investigations".

The conference participants discussed sharing experience, innovative approaches to education, and elaborated proposals for improvement of the AML/CFT and LEA personnel training system in the context of current challenges and threats.

Over **150 managers and officers of international organizations, government agencies and the European and Asian law enforcement research and educational centers** took part in the conference. The Forum was attended by the representatives of the **ITMCFM, Moscow and St. Petersburg Academies of the Investigative Committee of the Russian Federation, Physical Institute of the Russian Academy of Sciences, International Network AML/CFT Institute (INI), UNODC, OSCE, EAG, International Anti-Corruption Academy (IACA), Scientific and Educational Centre of the Prosecutor General's Office of the Republic of Azerbaijan, Cambridge Central Asia Forum, French National School for the Judiciary (ENM), Armenian Academy of Justice, Agency for Regulation and Development of the Financial Market of the Republic of Kazakhstan, etc.**

The International Network AML/CFT Institute and the International Training and Methodology Center for Financial Monitoring delivered two presentations at the conference:

1. "Analysis of Cryptocurrency Transactions for Combating Illegal Drug Trafficking" - the authors: Vladimir Glotov, Deputy Director of Rosfinmonitoring; and Alexey Yurov, Chief Specialist of Lebedev Physical Institute of the Russian Academy of Sciences.

2. "Network Cooperation in the Process of Personnel Training for National and International AML/CFT Systems" – the authors: Vladimir Ovchinnikov, Director of INI, First Deputy Director of ITMCFM; Ekaterina Butkeeva, Deputy Director of INI, Deputy Head of ITMCFM Educational Department; and Bella Safonova, Head of ITMCFM Department of International Relations.

In the framework of the conference, **the Agreement on Cooperation between the Academy of the General Prosecutor's Office of the Republic of Uzbekistan and the Moscow Academy of the Investigative Committee of the Russian Federation** was signed.

Following the results of the conference, it is planned to publish reports, presentations and research papers of the participants as part of the conference information package.

The conference focused on practical issues, facilitated the development of new online mechanisms for remote cooperation among the members of the International Network AML/CFT Institute and promoted establishment of professional contacts among INI's professors, students and practitioners.

Publisher

Autonomous Non-Profit Organization ITMCFM
Staromonetny Lane 31, bld.1,
Moscow, Russia, 119017. E-mail: info@mumcfm.ru.
Number of copies: 150.

Autonomous Non-Profit Organization ITMCFM

2020