FINANCIAL SECURITY

#41
MARCH/2024

PRESIDENT OF THE RUSSIAN ACADEMY OF SCIENCES

GENNADY KRASNIKOV:

"We are witnessing how scientific and technological innovation is transforming the world. Education in advanced technology and the application of our developers' and researchers' experiences are of paramount importance"

OPENING WORD

MR. YURY CHIKHANCHIN
Director of the Federal Financial Monitoring Service,
Chairman of Editorial Board

DEAR READERS!

We can hardly imagine the modern world without high technologies. They have permeated almost all aspects of our lives and have become integral to our daily activities. Thanks to financial technologies, we can make one-click purchases without visiting a store, transfer money, pay for services and apply for loans. This is convenient and time-saving.

Growing digitization has significantly impacted government's efforts. The Federal Financial Monitoring Service, like most other agencies, actively uses IT tools in its work.

The Service communicates with AML subjects via online personal accounts. We receive about one million messages from entities every day and respond within a few hours. Of course, processing this amount of information manually would be impossible.

However, let's not forget that there are people behind these technologies. Artificial intelligence, despite its immense potential, is only a tool to assist in solving complex problems. The ultimate decision is always made by humans.

As technologies evolve, the risks of their misuse for illegal purposes increase. Criminals adopt AI and other IT solutions, using them for embezzlement, money laundering, terrorism financing, drug trafficking, arms trafficking, and other illicit activities. At the same time, the extent of cybercrime has become transnational in scope.

That is why it is crucial to join efforts of the international community, public authorities, private sector and civil society in combating these new challenges and threats.

This journal covers the practices of applying digital tools and artificial intelligence by government agencies and banks in Russia and abroad, some aspects of regulating the financial services market, experiences in identifying and curbing cybercrimes and high-tech crimes, discusses topical issues of information security, and explores cryptocurrency use.

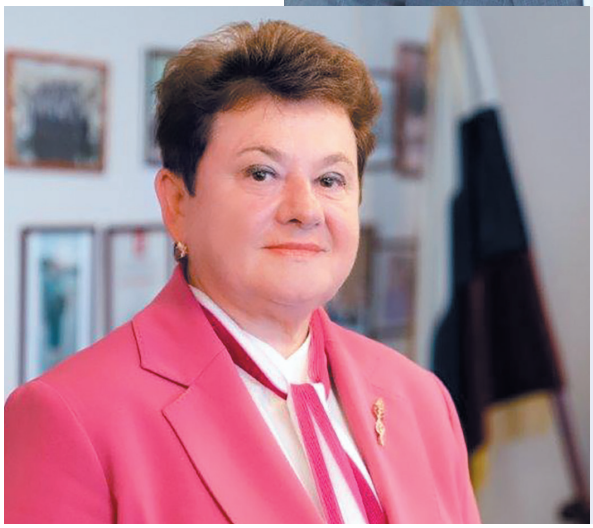
We invite readers to delve into the realm of high technology and reflect on its role in our lives.

CONTENTS

11 **MR KESHAV ANAND, MS. M. SHANMUGA PRIYA**
India's Fintech Ascendancy: Navigating the Intersection of Innovation, Financial Security and the Fight Against Cybercrime

14

YURY KOROTKY:
"Financial monitoring is a kind of financial tomography"



32

SVETLANA ORLOVA:
"Digital products and solutions are confident steps towards the development of public financial audit"

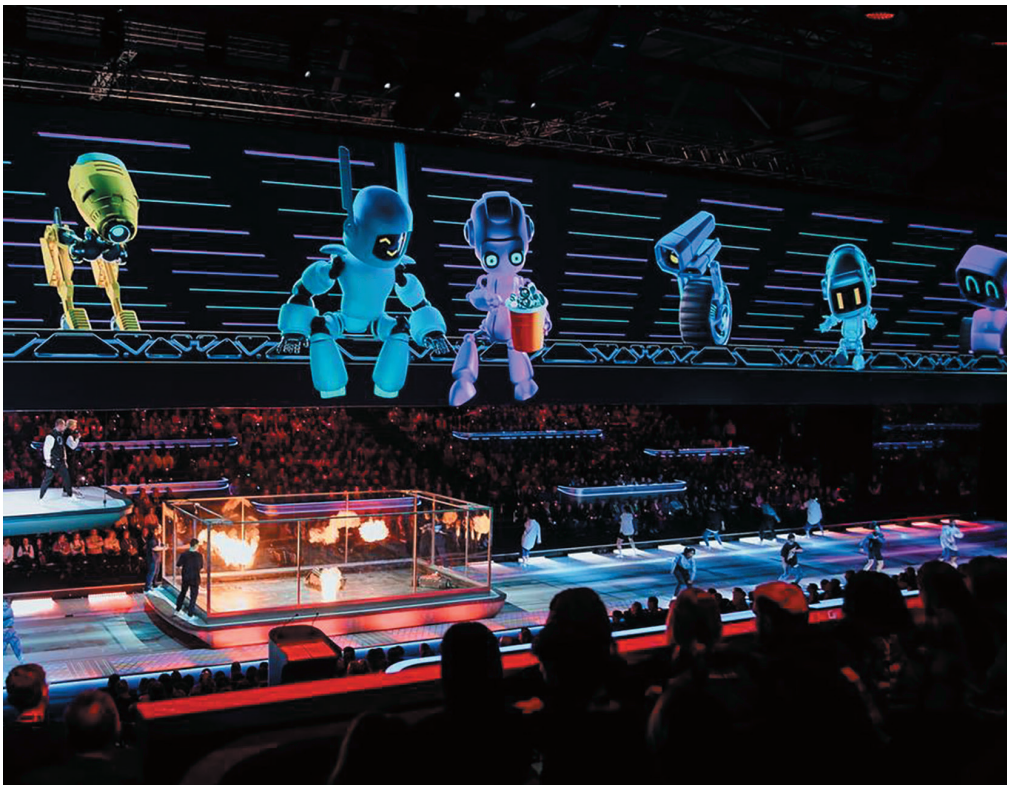
65 **OLGA TISEN**
Legal regulation of the circulation of virtual assets and combating their use for ML/TF purposes in individual EAG countries

Identifying and Combating Cybercrime

Cryptocurrency: Finding Solutions

Tribune of young specialists

Anti-Money Laundering News



80

"GAMES OF THE FUTURE" WINNERS OF THE FOUR CONTINENTS CUP TOURNAMENT VISITED KAZAN

WELCOMING SPEECH FOR FINANCIAL SECURITY READERS

GENNADY KRASNIKOV,
President of the Russian Academy of Sciences
Member of the Russian Academy of Sciences

DEAR READERS,

As we celebrate the 300th anniversary of the Russian Academy of Sciences, we not only honor our rich scientific history but also look ahead to the future. Our scientists are making strides on projects that will strengthen Russia's scientific and technological sovereignty, achieving significant milestones in the most advanced fields of science.

Today, we are all witnessing how scientific and technological advancement is transforming the world around us. Learning about new technologies and putting our developers' and researchers' skills to use in real-world applications are becoming increasingly important.

With this in mind, it's essential for the Financial Security journal to reach beyond its usual audience of specialists. It serves as a means for a wider readership to understand complex topics such as cybersecurity and the role of artificial intelligence in finance, including the associated risks.

Featuring articles by renowned Russian and international scholars, professionals, and public officials, the journal offers valuable insights into how the digitalization of the economy and finance is likely to progress in the future.

I extend my best wishes for your health and continued success.

HI-TECH FOR FINANCIAL SECURITY

COMBATING MONEY LAUNDERING AND TERRORIST FINANCING IN THE DIGITAL WORLD: CHALLENGE OF OUR AGE

The digitalization of all processes in our society is rapidly reshaping various industries and sectors, presenting both opportunities and challenges. The proliferation of digital technologies such as the Internet, mobile applications, cloud computing, big data, and artificial intelligence has revolutionized how people interact, work, and conduct business, including profound implications for the financial sector

ANTON LISITSYN,
Deputy Director,
Federal Financial Monitoring Service

Digital technologies also have a huge impact on the financial sector. Innovations such as online banking, mobile payments, e-wallets, blockchain technology, and cryptocurrencies have streamlined banking operations and opened up new possibilities.

Innovation and digital transformation are becoming key components in the development of countries in the digital economy, contributing to the creation of new industries and jobs, increasing productivity, and improving the quality of life. The integration of digital technologies in public administration makes it possible to simplify and automate processes, increase the availability of public services for citizens, improve the efficiency and transparency of public authorities, and adapt to changing conditions.

Artificial intelligence and automation hold immense potential for optimizing business processes and enhancing efficiency in the digital economy. AI facilitates the automation of routine tasks, enables the analysis of vast datasets, facilitates algorithm-based decision-making, and fosters the development of intelligent systems, ushering in a new era of data analysis and system intelligence.

Speaking about the digitalization of the Federal Financial Monitoring Service's activities, it should be noted that the Rosfinmonitoring Unified Information System development

concept addresses several areas where the application of artificial intelligence is justified and expected to improve staff performance.

Rosfinmonitoring's information system has amassed a substantial amount of data over the years, which is required for the implementation of analytical tasks.

However, data obtained from numerous heterogeneous external sources is frequently presented in an unstructured and informalized form, demanding additional processing or enrichment.

Processing of such data requires annotation, which enables the identification of business organizations for subsequent detection of signs of illicit activity, as well as feature space mapping for classification into risk categories.

The analysis of such large amounts of data is impossible without the use of machine processing. Rosfinmonitoring has created and successfully introduced a number of artificial intelligence technologies, including one that allows users to create, train, and use mathematical models to analyze corporate entities' behavior.

This technology includes a trainable classification model enabling the detection organizations with figurehead founders and CEOs among millions of business entities, as well as natural persons engaged in the cashing-out and other signs of suspicious or illicit activity.

The system also uses natural language processing to identify payment details in posts published on social media that exhibit indicators of fundraising for illegal purposes.

The entire Russian-language section of the Internet's global network is similarly analyzed. The technology extracts and reviews entities of interest to the Federal Financial Monitoring Service, identifying their interconnections.

The gathered data enriches Rosfinmonitoring's information repository by supplementing existing information about the entities.

In today's digital economy, the ability to collect and store massive volumes of data allows for the extraction of useful information, which plays an important role in decision-making, the development of new models based on hidden patterns and trends, and workflow optimization.

Rosfinmonitoring uses big data to deploy an international platform for financial intelligence units in seven countries: the Republic of Armenia, the Republic of Belarus, the Republic of Kazakhstan, the Kyrgyz Republic, the Russian Federation, the Republic of Tajikistan, and the Republic of Uzbekistan.

The International Money Laundering and Terrorist Financing Risk Assessment Center (IRAC), a technological platform initiated by Rosfinmonitring within the CIS countries, invites its partners to use innovative methods to coordinate and strengthen international cooperation in identifying and reducing the level of interethnic threats, which is becoming a critical aspect of work in the face of global turbulence.

Established to tackle ML/TF risks common to all nations through collaborative action, IRAC addresses issues such as suspicious transnational financial flows, the use of bogus organizations and entrepreneurs, cashing-out activities, transnational drug trafficking, and money laundering through international channels.

Combining information on financial flows of all member states within a unified information space enables a thorough examination of financial transactions in the CIS region. Furthermore, it ensures accurate forecasting of possible risks in order to implement joint preventive and protective measures.

Common risk perception, as well as technologically advanced and rapid data exchange mechanisms, will enable the Council of the Heads of FIU member states to efficiently respond to common risks, focusing efforts on combating crime and enhancing collaboration to counter illegal activities effectively.

"THE INTERNATIONAL MONEY LAUNDERING AND TERRORIST FINANCING RISK ASSESSMENT CENTER (IRAC), A TECHNOLOGICAL PLATFORM INITIATED BY ROSFINMONITRING WITHIN THE CIS COUNTRIES, INVITES ITS PARTNERS TO USE INNOVATIVE METHODS TO COORDINATE AND STRENGTHEN INTERNATIONAL COOPERATION IN IDENTIFYING AND REDUCING THE LEVEL OF INTERETHNIC THREATS"

A key objective of international interaction under the IRAC framework is to enhance the analytical capabilities of FIUs by utilizing data available in partner countries. Up-to-date information on the status and developments of cross-border financial transactions and the associated ML/TF risks enables international preventive operations involving FIUs and other national authorities of the Council of the Heads of FIU member states.

Another financial monitoring mechanism defending national interests is the National Financial Security Zone. In this case, Big Data technologies serve as a decision-support tool, along with the associated methodological tools, software, and hardware required for qualitative control system enhancement. The National Financial Security Zone is a system that combines a variety of methodological approaches to information systematization and processing, data analysis techniques, and hardware and software solutions for information storage, analysis, and visualization.

The National Financial Security Zone addresses several challenges, including:

- Data analysis in different areas;
- Identifying linkages between different areas of monitoring and gaining new insights;
- Application of gathered information to the quick implementation of preventative, protective, and blocking measures.

In essence, this is an interdisciplinary analysis of events in various areas of monitoring. It aids in the identification of risk concentration points and emerging risk factors. This system can be integrated into strategic planning processes to serve as a foundation for risk mitigation measures.

Blockchain technologies have revolutionized corporate practices and reinstated trust in the digital economy by ensuring the security and transparency of cryptocurrency transactions. However, a significant challenge arises from the inability to identify transaction participants despite the availability of source data such as cryptocurrency sender/recipient addresses, transaction time, and amount.

To address this issue, Rosfinmonitoring has adopted the Transparent Blockchain service, allowing for the analysis of cryptocurrency transactions based on data annotations of cryptocurrency market players. This enables monitoring and tracking of their behavior, enhancing oversight and regulatory capabilities in the cryptocurrency sphere.

Despite being a relatively new offering, Transparent Blockchain has garnered substantial interest, with over 7,000 users from Russian law enforcement agencies and foreign financial intelligence units accessing the service. Rosfinmonitoring has demonstrated successful financial investigations in collaboration with law enforcement agencies, resulting in the initiation of new criminal cases to combat cryptocurrency-related illegal activities.

Work is currently underway to ensure the uninterrupted operation of the service and its rapid development. It has the potential to become one of the most important components of Rosfinmonitoring's digital ecosystem.

The rapid advancement of digital technologies entails new requirements to education and skills necessary for successful adaptation and professional development in our ever changing world. In this landscape, digital literacy emerges as an indispensable component of education, encompassing the proficient use of digital tools, information processing, data handling, and problem-solving in digital environments. Educational programs should be more adaptable and flexible in order to train students in pertinent knowledge and skills. Curricula and teaching methods must be updated to match the most recent developments and requirements of the digital economy.

In light of these developments, Rosfinmonitoring recognizes the growing importance of recruiting talent with expertise in key areas essential for success in the digital era. This includes proficiency in machine learning, data science, Python programming, and other relevant disciplines critical for navigating the complexities of modern technology and driving innovation.

INDIA'S FINTECH ASCENDANCY: NAVIGATING THE INTERSECTION OF INNOVATION, FINANCIAL SECURITY AND THE FIGHT AGAINST CYBERCRIME

The digital and mobile banking sector in India has experienced remarkable growth in recent years, spurred by government initiatives that foster financial inclusion and leverage advancements in internet reach and the widespread availability of affordable smartphones

MR KESHAV ANAND,
Deputy Director, FIU of India

MS. M.SHANMUGA PRIYA,
Joint Director, FIU of India

The annual surge of technocrats and financial experts from India's prestigious universities and colleges, coupled with favourable government startup policies and the nation's solid GDP growth, has cultivated a vibrant ecosystem that lays the groundwork for the swift expansion of fintech startups.

A significant boost came with the introduction of the Unified Payments Interface (UPI) — a mobile-based, instant payment service — which saw the number of transactions soar from 672 million in January 2019 to a staggering 12,203 million in January 2024, with the transaction value skyrocketing from 109,932 crore INR (approximately 15.5 billion USD) to 1,841,084 crore INR (roughly 221.5 billion USD) over the same timeframe[1].

Despite the advancements and the democratization of financial services among the general populace, the rise of fintech has also introduced new risks to financial stability, particularly the increased potential for cyber-

[1] https://www.npci.org.in/what-we-do/upi/product-statistics.

financial crimes. The regulatory bodies, law enforcement agencies, intelligence organizations, and the fintech industry themselves are cognizant of these risks. Collaborative efforts are ongoing to confront these issues, implement remedial actions, and foster preventive awareness.

ANONYMITY, CONNECTIVITY AND THE RISE OF CYBERCRIME

Cybercrime is accelerated by the anonymity afforded by advancing technology and the internet. Individuals with even minimal technical skills can now illicitly earn money from the confines of their homes. Despite robust cybersecurity measures, certain system vulnerabilities remain open to exploitation. Cyber-attacks capitalize on these flaws, and covert tracking can reveal such invasive tactics. With the interconnectedness of computer networks, cyberspace allows for virtually unimpeded global reach.

FINANCIAL STABILITY RISK

In November 2022, India's National Risk Assessment revealed that cyber frauds and security flaws pose significant risks to financial stability, particularly affecting banking operations, credit, payments, securities, and money markets. Cyber frauds not only damage banks' reputations but also introduce several risks, including business disruptions, resource limitations, financial losses, and potentially liquidity issues. The growing instances of cyber fraud have recently emerged as a significant threat to the financial sector from AML vulnerability perspective.

CYBERCRIME TRENDS: FINANCIAL FRAUD ON THE RISE

According to the I4C's[2] Cyber Pravaha report for the second quarter of 2022, cybercrime incidents reported through India's National Cybercrime Reporting Portal (NCRP) surged to 237,658 from 97,179 in the same period the previous year. 'Online Financial Fraud' emerged as the dominant category, constituting 67.9% of all reported cybercrimes. Among the payment platforms, fraud related to Unified Payments Interface (UPI) saw the sharpest rise, escalating from 18,864 cases to 84,145 for the second quarter year-over-year. Additionally, incidents of debit and credit card fraud climbed significantly from 8,628 to 26,793, while complaints of internet banking fraud also saw a considerable increase, from 5,104 to 19,267 in the second quarter.

STRATEGIC ANALYSIS INSIGHT

The Strategic Analysis Group of FIU India conducted an extensive review of cybercrime-related suspicious transaction reports (STRs) from April 2018 to December 2022, noting a twelvefold increase in such reports. Predominant cybercrime types included credit card fraud, phishing, employment scams, identity theft, and fake loan/gaming/gambling apps.

A novel risk-based methodology was crafted to pinpoint and scrutinize individuals or entities implicated in cyber offenses. This method takes into account the variety of reporting entities that filed STRs, the frequency of these reports, and the array of predicate offenses cited.

Additionally, spatial analysis was employed to locate and address cybercrime hotspots for both preventive and responsive actions.

The results of this strategic and risk-based analysis have laid the foundation for action plans targeting high-risk groups associated with cybercrime. This includes operational analysis on such groups, training and ongoing dialogue with reporting entities to understand and address emerging cybercrime patterns, as well as to enhance anti-money laundering strategies in the face of rising cybercrime incidents.

RISK MITIGATION MEASURES

FIU of India is tackling cyber fraud and money laundering by collaborating with law enforcement agencies and financial entities to monitor fraud methods. A dedicated working group has updated and introduced Red Flag Indicators specific to cyber fraud, focusing on fraudulent transactions and schemes across a spectrum of deceptive applications, including those related to loans, betting, gambling, investments, employment, and romantic deception, among others. Enhanced measures now include monitoring application risks, KYC changes, IP address and geographical data to combat these crimes more effectively.

FIU of India, in collaboration with reporting entities, engages in vigilant and regular monitoring of applications, websites, and social media platforms that are known to exploit unsuspecting individuals via various cybercrime tactics. The intelligence collected through these measures is disseminated among the reporting entities, other intelligence agencies, and LEAs to prompt further

[2] Indian Cyber Crime Coordination Centre (I4C), is established by the Ministry of Home Affairs, Government of India to act as a nodal point to combat cyber crimes.

action. Furthermore, the analysis of progressive cybercrime strategies is utilized to enhance public awareness and to assist reporting entities in identifying and responding to such illicit patterns through their AML systems.

The RBI has also implemented several measures to mitigate risk and has issued advisories to banks on frauds and cybercrimes, outlining necessary actions. Specific advisories have been issued detailing the methods used by fraudsters, including the targeting of bank accounts and PPI (Prepaid Instrument) wallets, and advised banks to address these issues promptly by analyzing the fraud tactics and devising strategies to rectify detected deficiencies.

Further advisories were issued by RBI to banks concerning frauds and cybercrimes related to investment scams, part-time job offers, and ponzi schemes. The advisory emphasizes the need for

(a) a robust system to identify and monitor suspected money mule accounts,
(b) enhancing the KYC/AML processes including customer due diligence, name screening, risk profiling, real-time monitoring, and dealing with accounts potentially used for illicit purposes, and
(c) ensuring effective control and monitoring of digital transactions, including UPI, and reporting suspicious activities to FIU India, even when transactions are managed by third-party service providers.

INSTITUTIONAL INITIATIVES TO COUNTER CYBERCRIME

India's Ministry of Home Affairs has introduced the Indian Cyber Crime Coordination Centre (I4C) in 2019 to centralize the fight against cybercrime. The National Cybercrime Reporting Portal offers round-the-clock reporting, particularly for crimes against women and children. The Citizen Financial Cyber Fraud Reporting and Management System enables swift action against financial cyber frauds, backed by the '1930' helpline for online complaint assistance.

The CyTrain portal delivers online training for law enforcement on cybercrime investigation and prosecution, whereas, Joint Cyber Coordination Teams enhance inter-agency cooperation against cyber threats. The National Cyber Crime Forensic Laboratory provides advanced forensic capabilities to support crime investigations.

The Computer Emergency Response Team (CERT-In) addresses IT security incidents and promotes best practices. The Cyber Surakshit Bharat initiative educates government IT personnel on cyber threats and CyberDost raises cyber safety awareness among the populace.

In conclusion, FIU of India along with financial regulator and other anti-cybercrime arms of the Government of India strives continuously to prevent the incidence as well as reduce the financial damages occurring due to cyber frauds. The coordinated efforts between FIU of India, foreign FIUs and the regulated entities in terminating the flow of fraudulent funds to the illicit bank accounts of the cybercriminal has prevented the financial loss to scores of citizens and in turn safeguard the financial ecosystem of the country. With various visionary initiatives of the Government of India to combat cybercrimes, India is confident of erasing this menace in the near future.

FIU OF INDIA, ALONGSIDE RESERVE BANK OF INDIA (RBI) THE FINANCIAL REGULATOR AND SELECT BANKS, FORMED A WORKING GROUP TO TACKLE MONEY MULE ACCOUNTS IN CYBERCRIME, ISSUING GUIDELINES TO:

1. Standardize detection and prevention of mule accounts using risk assessments, KYC, and technological measures.
2. Promote information sharing between financial institutions to block fraud migration.
3. Introduce Behavioral Biometrics for better fraud detection.
4. Assign risk scores to accounts.
5. Create a network tracing framework for accounts in cyber fraud.

YURY KOROTKY:
"FINANCIAL MONITORING IS A KIND OF FINANCIAL TOMOGRAPHY"

Yury Korotky discusses the progress of Rosfinmonitoring information systems, the ideal IT system of the future and crypto compliance

Yury Korotky holds a Ph.D. in Law. He is an Honored Lawyer of the Russian Federation and an outstanding expert in the field of combating money laundering and the financing of terrorism

Having joined the Financial Monitoring Committee a year after its foundation, Mr. Korotky worked in financial intelligence for 22 years. Under his leadership, the organization expanded its analytical toolkit, designed and integrated new analysis methods and created a methodology for developing an AML/CFT risk management workflow.

In an exclusive interview with Financial Security, Yury Korotky discusses the evolution of the IT system in Russian financial intelligence, the most effective methods of high-risk analysis and the reasons why cryptocurrency turnover regulation is critical.

Mr. Korotky, having devoted over 20 years to Rosfinmonitoring, your contribution to the development of its information systems is paramount. Could you share how it all began?

Any information system (IS) is a combination of three components: information + equipment + "brains." In the language of information technology, it refers to an information resource, hardware and software and analytics. By the time I joined the Rosfinmonitoring Service is November 2001 (it wasn't even a Service at the time, but the Financial Monitoring Committee), the "information" and "equipment" constituents, i.e. the

system of collecting, storing and processing information, had already been largely formed. And it is only fair to acknowledge that I cannot take credit for this. I can't help but mention Alexander Yegorkin, Yury Grebenshchikov, Valery Makeshin, and so many more brilliant pioneers of our information system.

As for the third, analytical component, I was fortunate enough to make a significant contribution. It all started with a special accounting system. It was then known as SpetsDeloProizvodstvo ("Intelligence Workflow Management"). This system meticulously regulated the causes, grounds, as well as procedure of initiation and proceedings on financial investigations. In other words, we defined the algorithms for the complete analytical work process. This component remains relevant today, and, in fact, little has changed in more than 20 years. However, the name has changed to KOFR (Financial Investigation Support).

We are aware that you are the author of an AML/CFT risk management workflow design approach. One of its key messages is context-dependent risk assessment. Could you elaborate on its advantages?

I'll tell you more. In my opinion, this approach isn't just advantageous but essential. It recognizes that it's not the transaction itself that's suspicious but the circumstances surrounding it. As a result, only the environment in which the transaction takes place allows us to assess its suspiciousness. I believe this conclusion is pretty obvious. For example, in order to assess the suspiciousness of transactions in the public sphere, it is necessary to examine the details of the public contract, the pricing mechanism, the specifics of the bidding procedure, the validity of the supplier selection, the contractor's possible affiliation with the customer, and many other aspects that represent the context of public fund spending.

"THE IT SYSTEM OF THE FUTURE WILL RESEMBLE THE TECHNOLOGY OF AUTOMATED MULTIBAND IMAGING OF THE OPERATING ENVIRONMENT WITH HUNDREDS OF INDICATORS AND BIG DATA"

Financial Intelligence is an agency that requires advanced financial information technology since it analyzes a huge amount of data on a daily basis. What characteristics should a system possess in order to respond swiftly to challenges and threats? Is rapid system adaptability possible?

Yes, the ability to quickly adapt to changes in the surroundings and respond to continuously changing challenges and threats is a vital requirement for the system. And yet it's not enough. This kind of system is bound to perpetual "catch-ups" and delayed responses. The system must be proactive. Proactivity, achieved through context-based analysis and predictive analytics, allows us to anticipate threats and respond preemptively. We don't know what the criminal will do tomorrow or who they are. But we do know where they are most likely to show up. I can't reveal all of the secrets and risk indicators that allow us to identify areas of intensified monitoring, where the system is looking for specific signals and facts even before they exist and is ready to respond to them. Waiting for the enemy in an ambush is a proactive measure. However, it requires predictive analytics.

What would be the perfect IT system of the future for strengthening the anti-money laundering system?

Are you inviting me to dream? I notice a lot of parallels between the objectives of the financial monitoring system and computed tomography

in medicine. Fundamentally, both aim to diagnose a disease as soon as possible or to recognize its symptoms. Financial Monitoring is a sort of financial tomography. The IT system of the future will resemble the technology of automated multiband imaging of the operating environment with hundreds of indicators and big data. And, just as in medicine, the results will include health evaluations, diagnoses, and a treatment plans — all of this with the help of artificial intelligence. How do you like this vision of the future?

Sounds exciting and promising. In your opinion, which tools are the most useful for assessing the country's external threats and internal vulnerabilities?

In short, no single tool can do this. We require a set of tools and a system for automating the selection of tools configured for a specific type of identified threat/vulnerability as well as the specifics of the area where this threat/vulnerability exists.

Can you pinpoint prevailing trends in the development of IT systems for monitoring purposes?

There is a lot of talk about digitalization. During my chief digital officer training, one of the instructors stated that even a dump could be digitized. But then, rather than digitalization, you get a digital dump. And this is true. Transformation must first occur in the minds of those whose work should be digitalized. There is a concept known as digital maturity, which the system and its users must acquire. This process cannot be bypassed or avoided. However, it is possible and necessary to accelerate the process. I believe we are currently at the stage of digital maturation. How do I know it? Our Concept incorporates three major trends, and I'm not going to reinvent the wheel here. They include;

- Understanding and formalizing the structure of the AML/CFT scope (ontology);
- Process-oriented approach, i.e. a step-by-step description of the process of reaching the ultimate results and performance targets;
- Transition from data management to knowledge extraction and management.

From the "dilating pupil" approach to automation: which modern strategies for analyzing high-risk operations do you believe have shown to be effective?

With irony and a chuckle, we recall the "dilating pupil" approach, which we applied when we first started analyzing the incoming message stream. The underlying principle, however, hasn't changed. Both then, 20 years ago, and now, the strategy is based on what we call risk indicators. The distinction lies in the fact that formerly, an analyst's eye would respond to them. However, current information technologies enable not only the detection of risk signals, but also the calculation of scores, the mapping of areas based on their risk levels (the so-called traffic light model), the generation of heatmaps of the operating environment, and the identification of red zones. The risk matrix we designed has not yet been fully incorporated in situational analysis and national risk assessment, but I am confident that it is the future, and it allows plenty of room for the employment of artificial intelligence.

Rosfinmonitoring continues to interact with "friendly countries" and expands the geography of cooperation. Nevertheless, the IT systems of financial intelligence agencies differ. What are the primary means of fostering interaction, including the use of new technical products, within the framework of national specifics? Can information technology serve as a tool for strengthening collaboration?

The sequence here is as follows: first, collaborative work algorithms are established, and then a regulatory framework is altered to align with them. Only then can we work on joint IT initiatives. So, in this scenario, the key aspects are commitment and joint developments. IT specialists will not disappoint us as long as this sector is streamlined. The technical challenges of adapting and integrating different systems are significant, but not impossible. The key thing is to provide a unified operating environment and consistent approaches to its development.

> **"THE RISK MATRIX WE DESIGNED HAS NOT YET BEEN FULLY INCORPORATED IN SITUATIONAL ANALYSIS AND NATIONAL RISK ASSESSMENT, BUT I AM CONFIDENT THAT IT IS THE FUTURE, AND IT ALLOWS PLENTY OF ROOM FOR THE EMPLOYMENT OF ARTIFICIAL INTELLIGENCE"**

How do you see compliance evolving in light of the need to regulate cryptocurrency assets?

Compliance is about rules and regulations. Therefore, the development of the compliance system in the sphere of cryptocurrency turnover is directly dependent on how quickly we arrive at a fully functional system of cryptocurrency market regulation. At the moment, since compliance predominantly operates in the realm

of fiat money, we must enhance the existing internal control system with methods and instruments for disclosing the links between clients' banking operations and cryptocurrency transactions. We must learn to discover these ties using methods such as bank drops, P2P payments, and other connections between the two operating systems: fiat money and cryptocurrencies. Currently, we are actively implementing these measures in accordance with the President of the Russian Federation's directives as part of the Transparent Blockchain Project.

As for the prospects for regulating the domestic cryptocurrency market, I believe that rather than forcing crypto transactions into shadow circulation, we should try to boost their transparency. Another important area is cryptocurrency brokerage. In this regard, we must replace foreign virtual asset service providers (VASPs) with domestic cryptocurrency services markets that have their own crypto-compliance systems. Leveraging our previous success in onshoring major foreign IT vendors to ensure compliance with Russian legislation, including tax and anti-money laundering stipulations, we can now apply similar strategies to non-resident VASPs. The unregulated operation of foreign crypto-exchanges in Russia falls beyond Russian jurisdiction, or rather, within the "regulatory gaps" of Russian legislation. This scenario poses significantly greater risks than the inherent risks associated with cryptocurrencies themselves. Addressing these regulatory gaps is a task that demands prompt attention, but is taking an unacceptably long time.

"AS FOR THE PROSPECTS FOR REGULATING THE DOMESTIC CRYPTOCURRENCY MARKET, I BELIEVE THAT RATHER THAN FORCING CRYPTO TRANSACTIONS INTO SHADOW CIRCULATION, WE SHOULD TRY TO BOOST THEIR TRANSPARENCY"

FINANCIAL TECHNOLOGY MARKET REGULATION IN THE AML/CFT CONTEXT: UZBEKISTAN'S CASE

OTABEK RAKHMANOV,
Deputy Director of the Central Bank of the Republic of Uzbekistan

Uzbekistan's total population is 36.5 million people. 25 million of them are young people aged 15 and older, constituting a significant portion of the population. Given that young people are more likely to adopt new digital solutions, this presents a promising foundation for expending the use of financial technologies

FINANCIAL TECHNOLOGY MARKET OVERVIEW: ENTITIES

There are 35 banks on the market, with a total of 2,510 branches and offices that offer banking services. This provides widespread coverage of the country's territory as well as the population's access to financial services.

There are 49 payment companies in Uzbekistan, indicating a wide range of financial services available. In addition, there are twelve electronic money systems and six e-payment systems, contributing to market diversity and healthy competition.

Three payment system operators provide the necessary infrastructure for streamlined money transfers and transactions.

This highlights the significance of Uzbekistan's financial sector and illustrates that the country has a well-developed infrastructure for diverse financial operations, fostering the growth of financial innovations.

FINANCIAL TECHNOLOGY MARKET OVERVIEW: FACILITIES

The country has around 427,000 points of sale (POS), reflecting the widespread utilization of non-cash payment systems in retail and commercial establishments.

The number of ATMs and information kiosks exceeds 24,000 units. This suggests that financial services are easily accessible to the general public, as such facilities are frequently

located in both bank branches and public areas.

There are 42.4 million payment cards in circulation, indicating that electronic payment methods are widespread in the country. This increases consumer convenience and driving the growth of non-cash transactions.

International payment systems, including Visa, UnionPay, and Mastercard, account for 6.7 million of all payment cards. This demonstrates that the Uzbek financial system is integrated into the global economic context and facilitates international transactions for residents and businesses.

Therefore, Uzbekistan has a diverse set of financial technology facilities, enabling a wide range of services on both a national and global scale.

FINTECH MARKET: REGULATORY FRAMEWORK

The financial technology market in Uzbekistan is governed by a set of rules and regulations designed to ensure security and counter criminal activity. One of the key documents is the Law of the Republic of Uzbekistan No. 660-II on Anti-Money Laundering, Countering the Financing of Terrorism and Proliferation Financing dated August 26, 2004. This law outlines primary measures for combating financial crime and establishes criminal liability.

The Resolution of the Cabinet of Ministers No. 402 dated June 29, 2021 sets forth additional steps to reinforce the aforementioned law. This demonstrates ongoing enhancements of the legal framework in this area. These measures include specific provisions and instructions to counter money laundering, terrorism financing, and proliferation of weapons of mass destruction.

An integral component of regulation is internal control rules approved by the Central Bank and the Financial Intelligence Unit. These guidelines, tailored for banks, payment system operators, electronic money system operators, and payment organizations, aim to strengthen measures or countering financial crimes.

To ensure transaction security and customer identification, the Central Bank issued Regulations on Digital Customer Identification No. 3322 dated September 30, 2021. These regulations facilitate effective customer verification in online transactions, thereby mitigating the risk of financial fraud.

NEW FINANCIAL TECHNOLOGIES: STAGES OF ADOPTION IN CORPORATE PRACTICE

The integration of new financial technologies into corporate practice is a multi-stage process necessitating meticulous planning and adherence to operational security and efficiency standards.

The first stage involves a product survey, which entails a thorough examination of its functions, capabilities, and possible benefits to organizations and customers. Subsequently, an evaluation of associated risks, threats, and vulnerabilities is conducted to fully understand its potential negative implications.

This is followed by a detailed risk analysis, assessing the likelihood of various threats and their potential impact on business and customers. The analysis findings are used to develop risk mitigation strategies, which may include adjustments to the product, its applications, or the company's security policies.

Prior to product launch, notifying the Central Bank is imperative to ensure compliance with relevant legislation and financial market regulations. After receiving the notification, the Central Bank can conduct its own examination of the product and may provide recommendations for enhancements or additional security measures.

Finally, once the recommendations and approval from the Central Bank are received, the new product is introduced to the market. The process, however, does not end there. Organizations regularly review ML/TF risks associated with existing and new products at least once a year. This enables swift adaptation to environmental changes and facilitates adjustments to security and risk management policies.

FINTECH: DIGITAL IDENTITY SOLUTIONS

Financial technologies are critical to assuring the security and efficiency of financial transactions, with digital identity being a fundamental component of that process. Uzbekistan has developed and implemented national digital ID solutions to authenticate its residents.

One of the vital digital ID mechanisms is known as Liveness Detection. It protects against spoofing by utilizing deep neural networks to determine whether the photo displayed belongs to real-life individuals.

Another major approach is Face Recognition, which compares one

face to all images of faces stored in the database. This method allows for the identification of a single person amid a group, thereby increasing identification accuracy.

Face Comparison is yet another essential method, which determines whether faces in two separate photographs belongs to the same person. This approach is extremely beneficial for authenticating identity across various photographs or images.

The digital identity process can employ a variety of approaches, including automated processes devoid of human involvement, as well as those involving human participation. In both scenarios, high accuracy and security of the identification process are critical to protecting client interests and ensuring regulatory compliance.

FINTECH: SUSPICIOUS TRANSACTION THRESHOLDS

The Internal Control Rules for Anti-Money Laundering, Countering the Financing of Terrorism and Proliferation Financing (AML/CFT) in the Republic of Uzbekistan establish a number of specific thresholds and criteria for identifying suspicious financial transactions. The Rules are intended to ensure the security of financial transactions and prevent their exploitation for illicit purposes.

PAYMENT INSTITUTIONS

In Uzbekistan, the payment institution industry employs a wide range of measures and tools to mitigate the risks of money laundering and terrorist financing (ML/TF). These efforts aim to uphold the security and reliability of the national financial system, incorporating methods and procedures such as:

CDD (Customer Due Diligence) and KYC (Know Your Customer) systems: These solutions enable the identification of customers and their examination for compliance with regulatory standards. These include e-KYC, an electronic customer control system that enables more efficient and rapid identification procedures.

Internal rules and procedures: Payment businesses establish internal rules and processes for their employees, agents, and subagents to adhere to when interacting with clients. These protocols include guidelines for handling high-risk customers, such as public officials (PO).

Transaction monitoring systems: Payment institutions utilize specialized monitoring systems to automatically trace and analyze customer transactions in order to detect any suspicious activity.

Suspicious transaction detection and reporting systems: Payment institutions have mechanisms in place to identify suspicious transactions and report them to the appropriate supervisory and monitoring authorities.

Risk analysis and monitoring systems: Payment institutions regularly analyze, assess, and monitor transaction risks. They develop and implement risk mitigation solutions based on identified threats.

Development and update of internal rules: Payment institutions constantly review and update their internal policies and procedures to align with identified risks and legislative changes. This proactive approach enables them to successfully address new risks and regulatory requirements.

All these measures and tools contribute to the effective counteraction of money laundering and terrorist financing in Uzbekistan's financial sector, thus ensuring the stability and security of the national financial system.

ACCORDING TO UZBEKISTAN'S INTERNAL CONTROL RULES FOR AML/CFT, THE FOLLOWING ARE THE MAJOR THRESHOLDS FOR SUSPICIOUS TRANSACTIONS:

- Transfer of funds from a bank card to one or several bank cards or e-wallets using a mobile application, either once or multiple times within 30 days, for a total sum equal to or exceeding 500 times the Base Calculation Unit (BCU);
- Receipt of funds to a bank card from one or several bank cards or e-wallets, either once or multiple times within 30 days, for a total sum equal to or exceeding 500 times the BSU;
- Transfer of funds from five or more bank cards (e-wallets) to one foreign e-wallet using a mobile application, either once or multiple times within 30 days;
- Receipt of funds to five or more bank cards or e-wallets from one e-wallet, either once or multiple times within 30 days;
- Transfer of funds from one bank card or e-wallet to five or more foreign bank cards or e-wallets using a mobile application, either once or multiple times within 30 days;
- Receipt of funds from five or more foreign bank cards or e-wallets to one bank card or e-wallet, either once or multiple times within 30 days.

ELECTRONIC MONEY SYSTEMS

Electronic money systems are an integral part of Uzbekistan's contemporary financial infrastructure. According to national legislation, only banks are authorized to issue electronic money, enhancing reliability and oversight over electronic fund transactions.

However, in some cases, customer due diligence is not required, such as when an e-money transaction falls below a specific threshold (e.g. 1 BCU) or the total amount of e-money in the client's wallet is minimal (e.g. less than 5 BCUs). These exemptions are intended to streamline simple and frequent procedures while reducing the administrative burden on clients.

To mitigate risks associated with electronic money transfers, thresholds are established for both individual transactions and the total value of transactions over a given period of time. For example, an organization can set limits for a single electronic money transaction, the total amount of electronic money in a client's wallet, the total monthly value of electronic money transactions, and the total monthly value of card transactions. These measures enable banks and regulators to monitor and address possible hazards associated with the usage of electronic money while also ensuring the financial system's security and stability.

NEW FINANCIAL TECHNOLOGIES: NFC, QR CODES, TAP-TO-PHONE

Modern payment systems now incorporate new technologies such as NFC, QR codes, and Tap-to-Phone solutions, enhancing transaction speed and convenience, thus becoming preferred payment options for many users.

NFC payments are currently among the most common contactless payment options. The number of transactions using this technology has expanded dramatically in recent years, indicating its growing popularity. Thus, in 2021, the total value of NFC transactions amounted to UZS 12.2 trillion, increasing to UZS 31.6 trillion by 2023. Despite this, financial institutions must adhere to customer due diligence guidelines, especially for suspicious transactions. Infeasible due diligence requires institutions to notify relevant authorities and decline service to the customer.

QR CODE PAYMENTS ARE ALSO BECOMING INCREASINGLY POPULAR AS AN ONLINE PAYMENT OPTION.

The value and number of QR code transactions have skyrocketed in recent years. In 2023, there were 93,800 transactions, with a total volume of UZS 315 billion. This development necessitates a greater emphasis on security and fraud prevention, particularly among non-residents, POs, and customers involved in suspicious activities.

Tap-to-Phone technology enables mobile smartphones to function as POS terminals, reducing costs and increasing convenience for entrepreneurs. However, this calls for enhanced customer due diligence measures. This includes gathering information on fund sources, as well as examining payment purposes and the client's planned or completed transactions.

In general, the emergence of new financial technology creates new options for users but demands heightened vigilance from financial institutions regarding security and regulatory compliance.

NEW FINANCIAL TECHNOLOGIES: FACEPAY, ATTO, AND PALMPAY

The launch of a new contactless payment system in September 2023 marks a significant step forward in the sphere of financial technology. Known as FacePay, this technology offers a convenient and secure way to make payments using facial biometrics. Equipped with specialized cameras, FacePay recognizes users' unique facial features and promptly associates them with their linked bank card, ensuring data security and privacy.

Additionally, a contactless plastic card featuring NFC technology known as ATTO has been introduced to enhance payment solutions in the transportation sector. Available for purchase at dedicated ticket vending machines and point-of-sale locations, ATTO cards cater to a broad spectrum of users. This technology enables passengers to conveniently pay for travel services via a mobile application utilizing both NFC and QR code protocols, offering increased flexibility and ease of use.

Innovative banks have also rolled out pioneering payment mechanisms based on face and palm biometrics. For example, FacePay and PalmPay technologies enable clients to make payments and transactions at banking institutions by simply scanning their faces or palms. This not only enhances security but also streamlines the identification process, providing a seamless experience for clients who prioritize simplicity and convenience in their financial transactions.

DIGITAL TECHNOLOGIES IN SUPERVISION AND RAISING AWARENESS OF REPORTING ENTITIES

Digital technologies, including automated solutions for processing massive volumes of data, are becoming an essential component of supervision in countering the legalization of criminal proceeds (money laundering) and the financing of terrorism (AML/CFT). They allow for the deployment of a risk-based approach, the assessment of efficiency and communication with supervised entities, as well as the automation of individual business processes. Digitalization aims to improve the efficiency of interactions with supervised entities, reduce the administrative load on businesses, and free up supervisory authorities' resources

VICTORIA KAPARCHUK,
Advisor to the Monitoring Department, Federal Financial Monitoring Service

YANA BAYRACHNAYA,
Leading Expert of the Monitoring Department, Federal Financial Monitoring Service

ALEXANDER KURIANOV,
Head of the Monitoring Department, Federal Financial Monitoring Service, Ph.D. (Economics)

Over the past decade, there has been a dramatic five-fold increase in amendments to credit and financial sector laws, leading to heightened accountability among market participants. Fines for noncompliance with obligatory regulations are increasing in severity and frequency. RegTech (Regulatory Technology) solutions contribute to optimizing the process of complying with obligatory requirements in the setting of an ever-growing number of regulations. The period between 2017 and 2019 witnessed significant advancements in RegTech, coinciding with both increased regulatory demands and the rapid development of artificial intelligence technology.

Experts point out a number of benefits of RegTech solutions:

Improved efficiency
Technologies can rapidly process vast amounts of data, such as analyzing raw legal texts and extracting the information required for supervisory purposes.

Enhanced accuracy and completeness

Manual segregated processes often result in compliance gaps and human errors, amplifying regulatory risks. RegTech implementation bridges these gaps and ensures adherence to regulatory standards with greater precision.

Consistent and harmonized ecosystem

Technological tools foster transparency throughout an organization, integrating previously segregated processes and staff. This results in a unified information ecosystem that connects multiple units within an organization. This allows for faster data exchange which also leads to improved levels of compliance.

Effective risk management

Many RegTech technologies help effectively mitigate various types of risks, such as market abuse, cyberattacks and fraud, by monitoring and flagging suspicious behavior.

SupTech (Supervisory Technology) solutions also help optimize the fulfillment of statutory obligations.

SupTech refers to the use of digital tools, including hardware and software, by regulatory and supervisory authorities to implement their functions[1].

The increasing intensity and volume of both structured and unstructured data is driving demand for technologies capable of gathering, storing, analyzing, and visualizing various information arrays. Thus, in addition to standard reporting forms from reporting entities, competent agencies actively utilize open-source information (e.g. social media posts) to enhance their knowledge.

As regulating, supervisory, and law enforcement authorities rely on data, internal procedures, work tools, as well as human and other resources, they all face similar challenges, albeit to varying degrees. These challenges are associated with poor data quality and time-consuming manual processes. SupTech solutions can assist competent authorities in addressing these issues by enhancing their capacities, efficiency and effectiveness in data collecting and analysis through automating of routine tasks, innovating analytical methodologies, and generating processed information.

While interpretations of SupTech may vary, the pioneering definition refers to supervisory practices concerning securities market participants. The OECD underscores the efficacy of SupTech solutions in detecting insider trading, market manipulation, and related malpractices.[2]

Currently, the SupTech concept is being explored for a broader range of supervisory applications, extending to authorities in charge of monitoring compliance with competition and anti-corruption regulations, etc. Experts note that by improving the supervisory, analytical, and law enforcement capabilities of competent authorities, SupTech ensures a positive impact on financial stability, market integrity, and consumer welfare[3]. SupTech tools also enhance supervisory agencies' data collecting and management capabilities, thereby improving data quality — a prerequisite for advanced data analysis.

The adoption of SupTech by supervisory authorities underscores several significant benefits, notably:

Improved violation detection capabilities

We observe a growing trend among supervisory authorities, particularly those overseeing the securities market, as well as antitrust and anti-corruption enforcement agencies, in utilizing SupTech tools to detect various crimes, including:

- Money laundering and financing of terrorism, insider trading, and other types of unlawful activities (such as illicit sales and fraud);
- Anticompetitive practices;
- Bribery and corruption abroad.

SupTech systems, including those based on artificial intelligence, are especially useful for these purposes, as supervision is based on the analysis of enormous amounts of detailed, time-sensitive, and unstructured data from diverse sources. Furthermore, since digital technologies contribute to the emergence of new forms of ML and TF, as well as unscrupulous practices in the financial market, fraud, and anticompetitive practices, there arises a pressing need for innovative detection and countermeasure tools.

Financial intelligence units leverage artificial intelligence methods to assess incoming information flow, as well as sort, combine, and prioritize

[1] Going Digital: Shaping Policies, Improving Lives / OECD Publishing. URL: Mode of access: https://doi.org/10.1787/9789264312012-en.

[2] Using digital technologies to improve the design and enforcement of public policies // OECD. URL: https://dx.doi.org/10.1787/99b9ba70-en.

[3] The Use of Supervisory and Regulatory Technology by Authorities and Regulated Institutions // Financial Stability Board. URL: https://www.fsb.org/wp-content/uploads/P091020.pdf.

data outlined in reports concerning suspicious operations and/or client activities.

Regulatory authorities deploy artificial intelligence tools to identify violations in public procurement and authenticate corruption allegations. For example, in Brazil, artificial intelligence is used to sort incoming corruption reports and determine which instances warrant further investigation. Additionally, it helps in identifying signs of irregularities in public procurement procedures prior to contract awards.

Enhanced efficiency in law enforcement operations

Artificial intelligence systems hold the potential to significantly enhance the efficiency of law enforcement endeavors, given the inherently time-consuming and resource-intensive nature of investigations and prosecutions. In this context, artificial intelligence proves invaluable for scrutinizing vast datasets and ensuring adherence to format and structure guidelines in submitted reports. Furthermore, these systems can analyze evidence utilizing machine learning techniques, such as Natural Language Processing. Particularly adept at standardizing procedures and automating repetitive tasks involving extensive data volumes, AI systems emerge as powerful tools in law enforcement.

Enhanced data collection

As obligatory reporting gets increasingly complicated, regulators face challenges associated with the collection of late and inadequate reporting data, which may impact their supervisory and monitoring capabilities. At the same time, reporting organizations incur significant reporting-related expenses.

To streamline data collection processes, regulatory agencies have recently begun to implement the so-called "pull reporting" mechanisms, which allow them to obtain data from regulated entities as needed. APIs significantly facilitate data submission by reporting entities, thereby reducing costs and enhancing communication between the stakeholders[4]. Supervisory agencies are now exploring ways to convert reporting instructions into machine-readable formats to automate regulatory reporting and further facilitate compliance.

Enhanced efficiency in data management

Validation, consolidation, and visualization are the three key data management objectives. Each of them refers to a certain target point of the data management cycle. Validation is the process of confirming that data is complete, correct, and consistent in accordance with reporting criteria. Consolidation is the process of aggregating data from diverse sources and formats, while visualization entails presenting information in a visual way[5].

Of particular interest are instances of SupTech and RegTech integration observed in the operations of supervisory authorities across different countries, including EAG member states.

Thus, the Financial Monitoring Agency of the Republic of Kazakhstan uses a Personal Account service on its portal to monitor the activities of primary reporting entities on a daily basis. This enables quick response to indicators of AML/CFT infringement. The Personal Account is used to send messages to the FIU, submit lists for targeted financial sanctions on TF, train primary reporting entities in anti-money laundering legislation, provide recommendations, checklists, analytical reports, and patterns, publish various AML/CFT reporting data, and provide feedback, among other things. The implementation of the Personal Account service has enabled enhanced interaction with the private sector, including streamlined document flow.

The Mexican CNBV (Comision Nacional Bancaria y de Valores), responsible for overseeing AML/CFT, is currently implementing a cloud

In a broader context, digital solutions find application across various AML/CFT supervision domains, including:

- Remote monitoring of supervised entities for the subsequent use of the obtained information in risk assessment models;
- Streamlining customer due diligence and risk assessment processes;
- Feedback and automated communication of risk assessment findings, as well as information on detected signs of obligatory requirement violations to supervised entities;
- Coordination of preventive measures, such as the publication of training materials, including video trainings, questionnaires, FAQ sections, etc.

[4] The Use of Supervisory and Regulatory Technology by Authorities and Regulated Institutions // Financial Stability Board. URL: https://www.fsb.org/wp-content/uploads/P091020.pdf.

[5] The Suptech Generations // di Castri, S. et al. URL: https://www.bis.org/fsi/publ/insights19.htm.

computing project aimed at managing extensive volumes of data pertaining to compliance with mandatory AML/CFT standards. This initiative offers increased storage capacity and flexibility, along with improved mobility and computational capabilities. Moreover, the platform facilitates the generation of both basic and advanced analytical viewpoints to bolster monitoring effectiveness and identify irregular behavioral patterns.

In Singapore, sophisticated IT solutions are deployed to evaluate enterprises based on their risk profiles. Assessing the inherent risk of banks often involves collecting aggregated data from each institution regularly to estimate their ML/TF risk levels. This is sometimes a time-consuming and resource-intensive process which requires comparisons of data across similar banks and extensive qualitative assessments.

Furthermore, the Singaporean supervisory authority collaborated with data analysts to compile an exhaustive list of ML/TF risk indicators, design a machine-readable form for data collection, and develop a risk assessment methodology for its continued consistent application.

Today, upon receiving the requisite data, each bank's ML/TF risk assessment and a report detailing the pertinent data driving the evaluation can be swiftly generated. This enhanced capability enables supervisory authorities to more accurately pinpoint higher-risk financial entities. Moreover, if a bank's risk profile undergoes significant unexpected changes, it triggers immediate supervisory action.

AML/CFT supervision in Singapore relies heavily on network analysis, with Suspicious Activity Reports (SAR) serving as one of the key data sources for this purpose. Network analysis techniques enabled supervisory authorities to create an analytical tool for identifying networks of entities and individuals linked by SARs submitted by various reporting entities over different periods. This information is cross-referenced with the corporate register's company information and profile, including details on business activities, management, and beneficial ownership. A network analysis of this multidimensional dataset assists regulators in identifying high-risk areas and selecting financial institutions for targeted supervisory interventions.

Technology can also influence how on-site inspections are conducted. Supervisory authorities, for example, utilize automated analytical tools to examine the entire pool of the audited organization's transactions over the past two to three years. The system eliminates the need for inspectors to manually review operational data for irregularities. Ultimately, this approach enables regulatory authorities to allocate greater attention to high-risk areas during inspections and facilitates communication with supervised entities and their management regarding risk management and internal control issues. This communication is often supported by citing relevant case studies.

In Tunisia, supervisory authorities employ Blockchain technology to assess the risk associated with cross-border cash movement and to conduct targeted oversight of enterprises. According to the findings of Tunisia's 2017 National Risk Assessment, international cash transit and smuggling are considered high-risk activities. As a result, Tunisian authorities, including the Tunisian FIU, the Central Bank, customs authorities, and the Ministry of Internal Affairs, collaborated with the private sector (banks and currency exchange offices) to create Hannibal, a national platform for data collection, storage, and joint analysis, based on Blockchain technology. The platform creates dynamic dashboards allowing for more effective analysis of ML/TF risks associated with cross-border cash movements. It also assists FIUs, law enforcement agencies, banks, and exchange offices in detecting and identifying cash delivery networks.

Similarly, Rosfinmonitoring prioritizes the development of automated systems for assessing the risks of supervised entities, alongside online services for interacting with the private sector. The Personal Account tool on the Rosfinmonitoring website is one of such RegTech solutions that connects over 60,000 reporting organizations (sole proprietors). Beyond facilitating communication with Rosfinmonitoring and submission of information on entities and individuals involved in terrorist activities and proliferation finance, the Personal Account serves as an independent control tool for raising awareness of risks and legal requirements, as well as altering the supervised entity's behavior in the AML environment.

A crucial component of this mechanism is a system that enables remote communication of risk assessment results obtained through remote monitoring. Such corrective measures have proven highly effective, offering increased coverage, minimal administrative costs, and flexible configuration of risk assessment criteria. As a result, several thousand reporting entities mitigate their risk of noncompliance with AML/CFT regulations annually, relieving administrative burdens

while reallocating supervisory resources toward complex analytical tasks requiring professional judgment and experience.

The Personal Account's functionality also focuses on enhancing entities' understanding of AML/CFT regulations, national risk assessment findings, emerging trends, and illicit schemes/patterns.

CURRENTLY, MORE THAN 60 TYPOLOGIES, INCLUDING THEIR IDENTIFICATION SIGNS, HAVE BEEN POSTED IN PERSONAL ACCOUNT.

Besides, distance learning has been implemented and a number of training courses have been posted. During the course, users can assess their knowledge through testing. It is possible to automatically provide clarifications of legal requirements on typical issues.

Following the expansion of communications with the private sector, the Personal Account for the Professional Community (associations, unions, etc.) was launched in 2022. Its functionality allows for the provision of materials related to the fulfillment of AML/CFT laws by reporting organizations, notification of events held for relevant professional communities, etc.

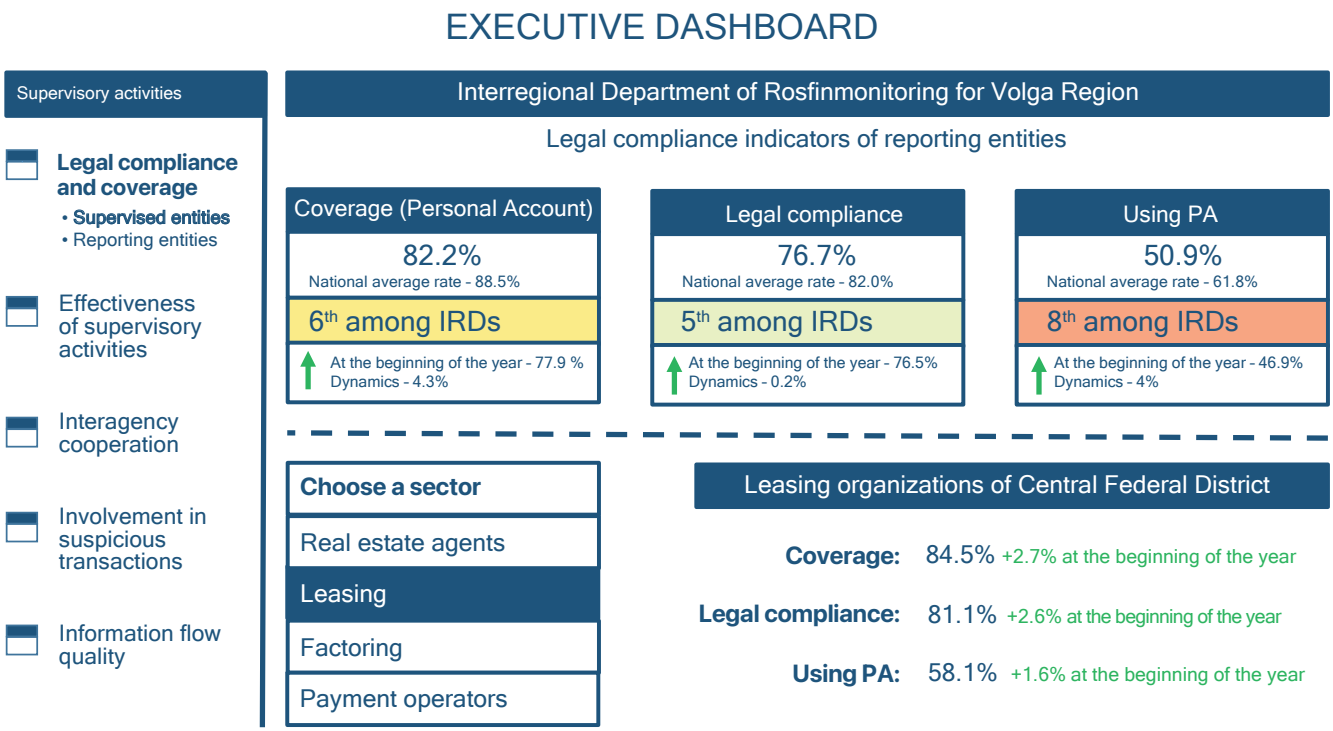
Additionally, an aggregator of customer information from diverse sources into a consolidated platform was created to localize the Personal Account for customer due diligence (CDD).

The supervisory authorities' Personal Account allows users to view the outcomes of Rosfinmonitoring's remote monitoring, ensuring quick responses from AML/CFT supervisory authorities to risks associated with supervised entities and promoting consistent approaches in supervisory planning. In addition, the platform provides real-time macro analytics, enabling the supervisory authority to monitor trends in the sector's compliance parameters, the involvement of its representatives in suspicious operations, and its exposure to specific risks. The Personal Account will soon undergo an upgrade to incorporate the Supervisory Authority Executive Dashboard.

Originally designed for the heads of Rosfinmonitoring's regional agencies (Figure 1), the Dashboard provides additional analytical data, including insights into the effectiveness of supervisory response measures based on various criteria such as supervisory tools, regions, and activity types. This allows to fine-tune a specific supervisory unit's operations by selecting the most effective approaches to supervisory activities.

The Personal Account can also be employed to get feedback. Starting in 2019, credit institutions provide feedback on suspicious transactions (STR) to reporting entities via the Personal Account on the Rosfinmonitoring website using the Information Flow Quality Index

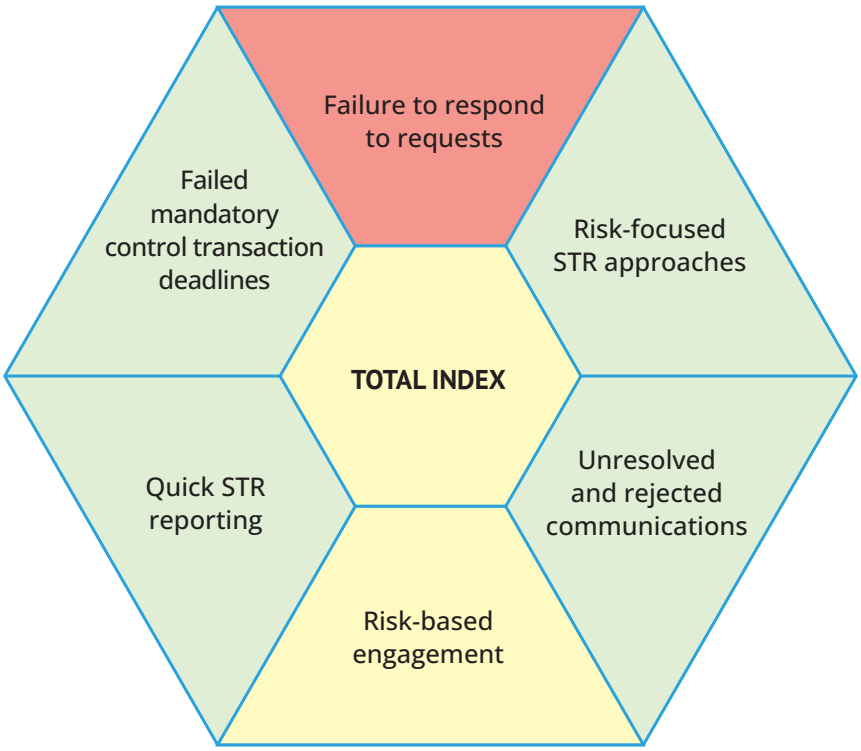
▶ Figure 1. Executive Dashboard



(Figure 2). Algorithms then generate an assessment based on the most significant criteria characterizing the effectiveness of communication between reporting entities and Rosfinmonitoring. Currently, the following information exchange parameters are assessed: the promptness of STR submission, the focus of incoming data on current risks, and the characteristics of interaction with the FIU (submission of information about risks (patterns), responses to FIU requests, and violation of FIU deadlines for information submission).

These criteria are then utilized to provide an integral assessment that characterizes the quality of communication between the entity and the FIU. As a result, we see faster identification of suspicious transactions, higher STR quality, and a better emphasis on risks.

▶ Figure 2. Information Flow Quality Index



Ensuring timely attention to current credit and financial sector risks and developments is crucial for enhancing the quality of information flow from reporting entities.

Credit institutions, for example, use the Personal Account to obtain information on the patterns and signs of suspicious transactions. In the context of AML/CFT, the term "pattern" refers to various systematic or recurring schemes for dubious transactions executed through financial institutions' infrastructure. As a rule, their systematic nature is associated with various vulnerabilities in the internal control systems of primary reporting entities.

Sources providing insights into new patterns include financial analysis findings from both FIUs and reporting entities. For example, Rosfinmonitoring cooperates with credit institution members of the Compliance Council (an advisory body to the Interagency Commission on AML/CFT) to regularly review financial analysis examples, which often serve as the foundation for patterns shared in the Personal Account. It should be noted that such information sharing about risks is also utilized to determine the Information Flow Quality Index.

Each pattern is assigned a unique number, enabling the electronic submission of STRs when a corresponding suspicious transaction is identified. Analyzing incoming reports enables Rosfinmonitoring to compile sample collections online, facilitating transaction flow analysis.

In general, the advancement of IT infrastructure enables supervisory authorities to reach a qualitatively new level of operation, expanding their expertise and expediting decision-making processes.

In the near future, the primary goal of digital technology development in supervision is expected to be the promotion of client-centric standards. This initiative aims not only to reduce regulatory burdens but also to foster a unique atmosphere of partnership and trust between the public and private sectors through more targeted communication efforts.

REGISTER OF BENEFICIAL OWNERS. KAZAKHSTAN'S EXPERIENCE

Pursuant to Article 6-1 of the Law of the Republic of Kazakhstan on Anti-Money Laundering and Countering the Financing of Terrorism, the Financial Monitoring Agency of the Republic of Kazakhstan is tasked with maintaining the Register of Beneficial Owners of Legal Entities (the Register)

DINARA MUSINA,
Head of the Operational Analysis Department, Financial Monitoring Agency of the Republic of Kazakhstan

The Register provides crucial information to various entities involved in monitoring compliance with anti-money laundering and counter-terrorism financing laws, including government bodies, law enforcement agencies, and subjects of financial monitoring.

In this article, we delve into the methodologies employed by the Financial Monitoring Agency to establish and administer the Register, alongside its personalized account features tailored for state regulators, law enforcement agencies, and subjects of financial monitoring.

BUSINESS PROCESS OF THE REGISTER OF BENEFICIAL OWNERS

According to FATF recommendations, information on beneficial owners must be complete, accurate, and up-to-date, so the most important element of the business process is collecting information from different sources.

THE DEVELOPMENT AND UPKEEP OF THE REGISTER ARE DRIVEN BY THREE PRIMARY FACTORS:

- Results of risk assessments conducted on legal entities, determining their involvement in predicate offenses and money laundering;
- the Agency's access to various databases and its technical capabilities for data processing;
- Adherence to updated FATF recommendations.

Therefore, the primary focus of the business process revolves around sourcing information from multiple channels. Initially, the process entails gathering data on beneficial owners as declared by legal entities. These sources include:

- **Ministry of Justice:** Central repository of registration data nationwide;

- **Subjects of financial monitoring:** obliged to document and register beneficial owners of their clients (e.g., register of major shareholders, register of beneficial owners managed by Astana International Financial Center);
- **State Revenue Committee:** Residents submit declarations regarding control of foreign companies as part of their tax obligations;
- **Financial Monitoring Agency:** Authorized to request and receive information on beneficial owners;
- **Ministry of Energy, Ministry of Industry and Infrastructure Development:** Authorized to receive and store information on beneficial owners of mineral developers, aligning with international transparency standards in the extractive sector.

The first step involves aggregating data on beneficial owners provided by legal entities from diverse sources. This information is predominantly accessible to the Financial Monitoring Agency through online platforms, with retrieval and consolidation processes automated.

OTHER SOURCES

To corroborate the retrieved data, additional information is sourced from various channels, including:

- Reports on threshold and suspicious transactions from subjects of financial monitoring;
- Tax returns from the State Revenue Committee;
- Family and corporate connections from the Ministry of Justice;
- Electronic invoices from the State Revenue Committee;
- Data from foreign FIUs, including history of requests;
- Open sources intelligence from the Internet.

STATUS OF BENEFICIAL OWNERS

A detailed methodology for processing this data to ascertain beneficiaries has been devised based on aggregate data. Automated algorithms are employed for data processing, with 19 algorithms currently operational and demonstrating effectiveness.

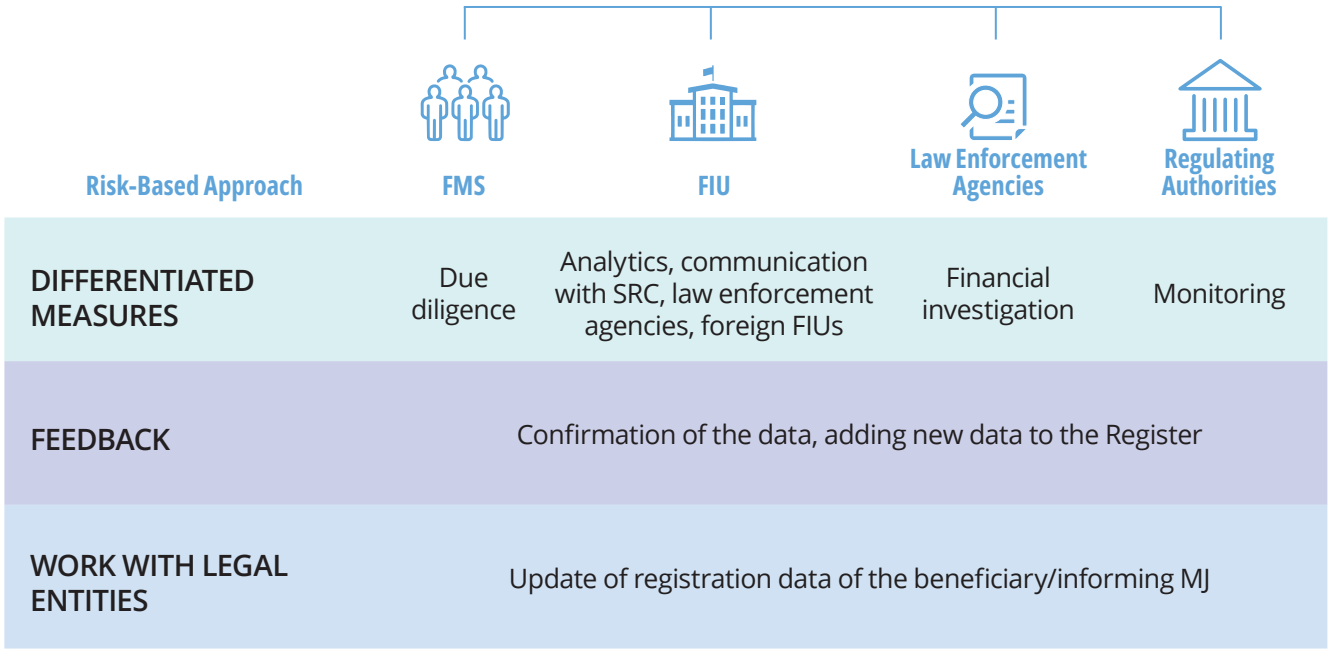
AS A RESULT OF THESE ALGORITHMS, INDIVIDUALS ARE CATEGORIZED INTO TWO STATUSES:

- **Registered beneficial owner**
- **Alleged beneficial owner**

Registered owners are those whose data is officially recorded in the Ministry of Justice; while all others are deemed alleged beneficiaries.

The algorithms for identifying alleged beneficial owners are meticulously created, each based on specific methodologies and information sources, and are assigned reliability scores ranging from 1 to 4, with 1 indicating low likelihood and 4 signifying high likelihood. Each algorithm operates on a scheduled basis, with results archived post-execution.

Feedback from anti-money laundering system participants is instrumental in refining and broadening existing algorithms.



USERS OF THE REGISTER INCLUDE PARTICIPANTS OF THE ANTI-MONEY LAUNDERING SYSTEM, NAMELY STATE REGULATORS, LAW ENFORCEMENT AGENCIES, FINANCIAL MONITORING SUBJECTS, AND THE FINANCIAL INTELLIGENCE UNIT. THROUGH THEIR PROFILES, USERS CAN CONTRIBUTE TO THE REGISTER BY:

1. Confirming or refuting the FIU's assumptions;
2. Proposing their assumptions, such as alternate alleged beneficial owners, along with detailed algorithms/ schemes.

Register's users are AML/CFT stakeholders: government authorities - regulators, law enforcement agencies, financial monitoring entities, financial intelligence units.

Additionally, as part of their client interactions and subject review/ monitoring activities, users encourage businesses to update their registration data.

By actively utilizing the Register of Beneficiaries, participants in the anti-money laundering system play a vital role in preventing and mitigating the involvement of entities in predicate offenses and money laundering.

ARTIFICIAL INTELLIGENCE AND FINTECH:
NOW AND IN THE FUTURE

SVETLANA ORLOVA:

"DIGITAL PRODUCTS AND SOLUTIONS ARE CONFIDENT STEPS TOWARDS THE DEVELOPMENT OF PUBLIC FINANCIAL AUDIT"

Svetlana Orlova, Auditor of the Accounts Chamber of the Russian Federation, discussed with the Financial Security journal the implementation of AI measures in government control (audit), the potential of new technologies to enhance public administration, as well as current digital solutions in the field

Svetlana, thank you for taking the time to talk to us. This issue covers, among other things, the development of artificial intelligence. How do you envision AI's role in government control/audit?

Firstly, I must highlight that our efforts align with the directive of Russian President Vladimir Putin, issued at the St. Petersburg International Economic Forum 2023. The directive emphasized the crucial role of active automation and the development of artificial intelligence technologies in the supply-side economy. Consequently, there is a concerted push to implement and leverage these advancements, support domestic big data software production, and initiate AI-based projects.

In February 2024, significant amendments to the National AI Development Strategy through 2030 were introduced by the Russian President. Notably, federal executive bodies are now tasked with aligning their activities with this strategy

when developing and implementing sectoral strategic planning documents. Consequently, the focus of federal executive bodies' work will, to some extent, shift towards artificial intelligence technologies.

The coherence of this strategy was reiterated in the Address of the Russian Federation President to the Federal Assembly. Over the past few years, the Accounts Chamber has been working towards this objective, primarily focusing on digitizing inspectors' activities.

Undoubtedly, some AI technologies are already prevalent in smartphones, healthcare, education, smart home systems, and industry. The significance of big data and its analysis through neural network technologies cannot be overstated in the development and utilization of AI.

As for the government financial audit, the quality of big data and especially their reliability hold particular importance. Consequently, our attention has been directed towards organizing big data analysis. Digital solutions developed by the Accounts Chamber, encompassing tools for data collection, analysis, and visualization (data analytics), have effectively addressed this challenge. As of the end of 2023, the Accounts Chamber's registry of digital solutions and products boasts more than 300 entries.

These solutions have propelled audits into a new era characterized by advanced technologies and methodologies. Moreover, they have significantly reduced the time inspectors spend analyzing audit data, minimizing human error and yielding more accurate results. Additionally, these solutions have expanded the scope of audited information considerably. This transformation of audit processes has been made possible through the Accounts Chamber's extensive efforts in digital transformation.

Within the domain of public administration audit, which I oversee, we are actively promoting digital transformation within audited entities as well.

Can you share the results of this work in more detail?

One notable example of our collaborative efforts is the advancement of IT adoption in court proceedings.

In 2023, we convened four extended meetings involving 15 leading ministries and agencies spearheading the digitization process, including the Russian Ministry of Digital Development, Communications and Mass Media, the Ministry of Justice, the Federal Treasury, the Federal Tax Service, the Federal Bailiff Service, and others. Together, we explored best practices for integrating modern technologies into court proceedings, enhancing interagency cooperation between government bodies and the judicial system, and refining the management of arbitration court deposit accounts.

These discussions culminated in a meeting with representatives from the Government of the Russian Federation, the Supreme Court, and the Federation Council of the Federal Assembly.

Towards the end of 2023, we participated in signing an agreement expressing the intent to develop unified approaches to the implementation of modern information and communication technologies in court proceedings and administration. Signatories included the Judicial Department of the Supreme Court, the Ministry of Digital Development, Communications and Mass Media, and the Federal Treasury.

This collaboration aims to create a user-friendly service for citizens and businesses integrated into the judicial process, simplifying payment processes, enhancing transparency, and mitigating potential misuse of funds. Currently, the project is in the IT solution development stage, with plans for piloting at the Moscow Arbitration Court. Upon successful implementation, measures outlined in the agreement will be extended to all federal courts and regional offices of the Judicial Department of the Supreme Court of the Russian Federation. Furthermore, in partnership with the judicial community, the Judicial Department of the Supreme Court, and relevant ministries and agencies, we are creating a shared roadmap for the adoption of digital solutions in court proceedings and interagency relations.

We will be directly engaged in several pilot projects:

- The judicial system, alongside the Ministry of Digital Development,

Communications and Mass Media, the Ministry of Justice, the Ministry of Finance, the Treasury, the Federal Tax Service, and the Federal Bailiff Service are actively working on a solution to **assign unique accrual identifiers (UINs)** in enforcement documents issued by the courts. While a temporary solution has been developed, significant coordination efforts are still required among all concerned parties in this area;

- The judicial system, in conjunction with the Treasury and the Federal Bailiff Service, is pursuing the potential implementation of a major and highly significant joint project — **the register for the enforcement of court decisions.** This model aims to enhance the transparency of enforcement proceedings and facilitate more effective electronic cooperation between government agencies and citizens.

"THIS COLLABORATION AIMS TO CREATE A USER-FRIENDLY SERVICE FOR CITIZENS AND BUSINESSES INTEGRATED INTO THE JUDICIAL PROCESS, SIMPLIFYING PAYMENT PROCESSES, ENHANCING TRANSPARENCY, AND MITIGATING POTENTIAL MISUSE OF FUNDS"

Can you provide examples of digital solutions and their positive results in improving public administration?

As the head of the department, overseeing the implementation of 18 digital solutions in 2023 alone, I would like to highlight several pivotal initiatives that have significantly enhanced the public administration system.

For instance, to facilitate the adoption of Methodological Recommendations for identifying and assessing corruption risks in audit and expert review activities utilizing AI technology, we developed the Software for Identification of Corruption Risks in Procurement from a Single Supplier. This software automatically verifies whether contracts comply with the Federal Law On Contractual System in Procurement of Products, Services, and Works for National and Municipal needs, thereby highlighting any nonconformities as potential breach risks.

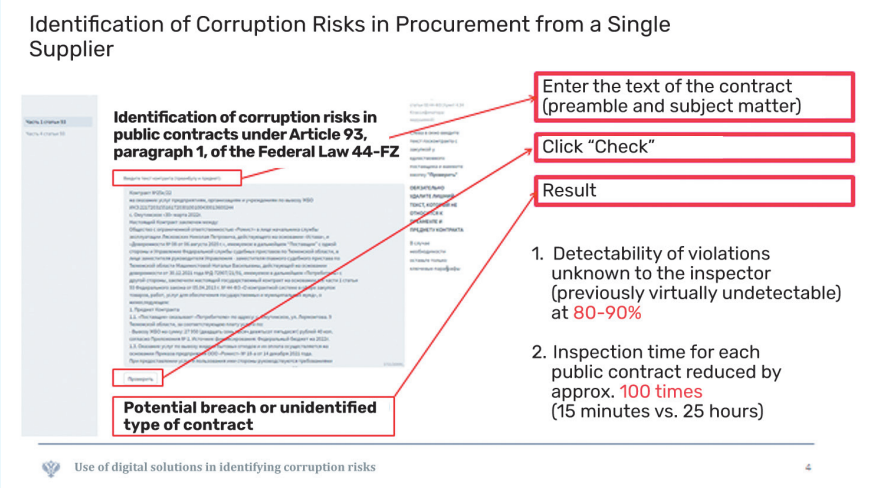
During the development process, we analyzed approximately 100,000 contracts from the Unified Information System, identifying deviations and potential risks. The project is now operational and accessible through the Accounts Chamber's internal portal. Another notable digital solution, developed as part of our expert review activity, focuses on analyzing the administration of personal (deposit) accounts for recording transactions with funds held by arbitration courts from 2012 to 2022 and in 2023.

The solution is designed to compare payment documents for funds deposited at arbitration courts with the number of cases submitted for review over the past 11 years, ensuring compliance with the Regulations on the activities of Federal Courts and Regional Judicial Department Offices concerning the management of personal (deposit) accounts and recording transactions with such funds.

With approximately 9 million payment documents and over 27 million arbitration cases, the sheer volume of data posed a monumental challenge.

Moreover, the data presented additional challenges due to its inherent vagueness. Discrepancies arose from diverse depositors and recipients, including individuals not affiliated with arbitration cases, and instances of incomplete data, such as records containing the Federal Treasury Department's Taxpayer Identification Number (TIN) instead of the court's TIN.

The implementation of the IT solution proved instrumental in overcoming these obstacles. Furthermore, it underscored the necessity for a pilot project aimed at streamlining and automating the management of funds deposited by citizens and organizations into Federal Treasury accounts in accordance with procedural legislation. This, in turn,



led to proposed amendments to the Regulations on the activities of Federal Courts and Regional Judicial Department Offices governing the management of personal (deposit) accounts.

What digital product are your employees currently using?

Today, we are in the final stages of refining a product developed in response to feedback from various departments of the Accounts Chamber, as part of the implementation of our Methodological Recommendations for identifying and assessing corruption risks. This product harnesses innovative generative artificial intelligence technology.

For those unfamiliar with this technology, allow me to provide a brief explanation: it offers the capability to train your own algorithm for information retrieval, aligning with predefined criteria. Once this solution undergoes refinement and testing, the analysis of public contracts will not only highlight potential risks but also offer detailed descriptions of these risks and a spectrum of potential underlying causes for breaches.

Furthermore, upon project completion, we anticipate the ability to analyze not only selected contracts but also to batch upload documents in any machine-readable format. This automated process of identifying risk areas promises to significantly reduce the time required for document processing and analysis.

It is crucial to underscore that while AI plays a vital role as an assistant in this process, it will not replace the role of a human inspector.

> ***"IT IS CRUCIAL TO UNDERSCORE THAT WHILE AI PLAYS A VITAL ROLE AS AN ASSISTANT IN THIS PROCESS, IT WILL NOT REPLACE THE ROLE OF A HUMAN INSPECTOR"***

ARTIFICIAL INTELLIGENCE IN FINANCE AND ITS IMPACT ON AML/CFT

V. DOSTOV,
Chairman, EMA Council; Ph.D., Mathematics & Engineering; Senior Researcher, Financial University

Artificial intelligence has arguably been the most significant breakthrough of the last two years. A qualitative leap in its development will surely allow us to reassess old methods for solving numerous intellectual challenges that previously required human participation, while also to broaden the spectrum of tasks that may be completed without human intervention

According to a recent advisory report of the Bank of Russia[1], the financial sector has become one of the most active adopters of this new technology. In this article, we will provide a quick overview of this pioneering technology and its potential impact on the evolution of the financial sector, particularly focusing on AML/CFT.

INTRODUCTION TO TECHNOLOGY

One article cannot provide a full account of a complicated technology like AI, which has a long history of development and use. Therefore, we will limit our discussion to the articulation of the key features of the major neural networks and the large language models (LLM) built upon them. However, the term "language" might be misleading, as for AI, any object translated into a sequence of ones and zeros, be it a book, a digitized photo, scoring data, cryptocurrency charts and fluctuations, videos, and so on, essentially constitutes statements in a specialized language.

Simply put, a neural network is a sequence of transformations from

[1] https://cbr.ru/press/event/?id=17177.

initial values (input vectors) into an output vector. For example, a typical LLM converts a source text (a column or, most typically, a row) of alphabetic characters into an output column (row). This article, for AI, is essentially a long column of letters. A user can submit it to AI as input, including a question column, and receive a Yes/No answer, thorough response, or translation into another language. A column of symbols can represent a wide range of objects, such as images, videos, research data, transaction sets, and so on.

The conversion process itself is surprisingly straightforward (a picture may be added here). Taking the first column, we transform it into the second using a simple rule: each cell in the output column is the sum of all the values in the first column multiplied by arbitrary aij coefficients forming a table (matrix). Furthermore, resulting values in each cell of the second column are converted using simple formulas that lower smaller values while increasing larger ones, so boosting the contrast of the outcome. Next, the same procedure is used to construct a third column with another Aij matrix, and so on until we reach the final value. Each layer comprises the coefficient matrix, the conversion formula, and the column. Remarkably, only a few layers are typically necessary. Thus, back in 1958, Rosenblatt demonstrated that a three-layered neural network was sufficient for any image classification task (number/letter recognition, car/pedestrian detection, and a variety of other tasks).

However, where does AI acquire its Aij matrices? The answer is simple: it requires training. This training process is quite straightforward. First, the coefficients are generated at random, and AI is provided an input string with a known answer, such as a Yes/No question with a predetermined response. AI returns an answer, which is initially random. If correct, it is asked another question. If the AI's output is incorrect, the matrix is slightly altered, and the inquiry is repeated. This is done multiple times until AI produces an accurate output. This procedure is repeated an infinite number of times until the proper output is achieved in the vast majority of cases, if not all. This is the point at which AI is regarded fully trained and ready for deployment in real-world scenarios.

> Humanity has long dreamed of creating artificial intelligence. Markov, a Russian mathematician, laid the groundwork for language models in 1913. However, it was not until 2022 that a critical mass of software, hardware, and contextual capabilities for training powerful artificial intelligence gained traction, and text and image processing models began to appear.

Furthermore, neural network-based LLMs have proven to be cross-functional. Historically, AI development took place in a wide range of seemingly unconnected fields. Thus, algorithms for text analysis differed greatly from those for gaming or drone control. Deep-learning neural networks turned out to be "omnivorous." They can tackle any type of problem when converted to data vectors. This allowed us to focus all of our efforts in one breakthrough direction. AI applications quickly spread to a wide range of fields, including digital art and medicine. The financial sector was obviously no exception.

AI IN FINANCE

Originally focused on language models, early AI models primarily targeted client communication tasks. These include support chatbots, request analytics, call center personnel management, and so on. Product description optimization also belongs to this category. Such AI applications use common language models, with financial specifics appearing only in certain contexts.

AI can also be used to analyze client behavior and optimize existing products. In this situation, training incorporates a variety of product attributes, such as those associated with deposits. AI learns to optimize these parameters to achieve desired outcomes, such as specific sales targets. While more ambitious attempts to analyze and optimize customer behavior have been made, regulating them has proven surprisingly challenging.

Scoring represents a separate area of AI work. By leveraging AI, institutions can rank consumers based on complex methodologies and correlations between multiple criteria, leading to more accurate loan issuance decisions.

The employment of AI in financial information security holds promising prospects. AI can analyze external queries to an automatic banking system (ABS) to discern whether they originate from legitimate clients or constitute hacking attempts. In this scenario, AI undergoes training on a vast dataset comprising genuine requests and attempted attacks.

This is only a short list of use cases, and the number of applications is ever growing.

AI IN AML/CFT

Analysts have long discussed the practical advantages of integrating AI in AML/CFT. In 2018, KPMG and the Association of Certified Anti-

Money Laundering Specialists (ACAMS) observed a significant increase in the use of AI to combat money laundering. The FATF echoed this observation in its scoping note[2]. We are currently seeing the following important areas for AI deployment:

1. Customer risk assessment prior to onboarding

In this scenario, AI is trained using a vast database of former bank clients (both legal entities and natural persons) whose characteristics are known a posteriori. Training makes it easier to rank consumers based on their risk level, thereby mitigating issues related to de-risking. According to Sber and HSBC, this approach enables the onboarding of a large number of customers who might otherwise face unjustified refusal under the standard review system.

2. Analysis of ongoing transactions

Traditional transaction analysis methods rely on established patterns such as payment splitting and consolidation, suspicious intermediates, and so on. Real schemes, however, are often more sophisticated than that, rendering formal analysis ineffective. AI goes beyond formal criteria and can be more successful in tracking and reporting suspicious transactions. VTB, Sber, Standard Chartered, JPMorgan Chase, Danske Bank, and other banks have already integrated such procedures. It is worth noting that such approaches are also useful for controlling distributed payment systems. In particular, in August 2020, Rosfinmonitoring announced the development of a prototype cryptocurrency transaction analysis system using artificial intelligence technologies. Dubbed the Transparent Blockchain, the system debuted in February 2021.

3. Affiliation graph building

The primary goal of AML/CFT is to identify hidden benefit and affiliation relationships between participants in complex payment structures. AI facilitates the analysis of both payment transactions alongside additional information such as entries in legal entity registers, information about owners from external sources, and so on. This enables the construction of graphs depicting nodes representing legal entities and natural persons, as well as affiliation linkages between the nodes. This aids in identifying formal and informal relationships among supposedly independent participants in payment transactions.

4. Human compliance monitoring

This model was initially tried in "human" call centers (such as JustAI solutions). A number of client requests are currently beyond the capabilities of AI. However, AI can analyze text and speech chats to deliver assessments and recommendations on human resource quality. Similarly, AI can monitor human compliance, detect common faults, rank workers based on quality and offer relevant recommendations.

5. Analysis of legislative amendments

There is hope regarding the use of artificial intelligence for automating the

[2] Opportunities and challenges of new technologies for AML/CFT https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Opportunities-Challenges-of-New-Technologies-for-AML-CFT.pdf.coredownload.pdf.

processing of regulatory documents. This could enable banks to optimize their internal policies in response to changes in regulatory requirements.

6. Contract review

Compliance operations require significant time investments in studying submitted documents to establish the source of funds and the purpose of transactions. This is a significant burden due to the intricacy and diversity of these documents. AI can alleviate this burden by examining documents to verify authenticity and compliance with transaction purposes.

7. Selection of basic indicators

As previously stated, AI has the potential to transform the compliance model by shifting from a fixed set of criteria to analyzing the full set of operations. Conversely, a reverse transition is possible — training AI on a set of suspicious operations to select a limited yet highly effective set of criteria for rapid analysis.

8. Identification

Another category of AI applications is linked with client identification. These applications are not specific to the financial sector, but rather applicable across industries. This includes examining client images and photographs in documents, analyzing speech and video recordings, and employing other approaches to enhance identification reliability, both remotely and in person.

AI VULNERABILITIES IN AML/CFT

Despite its numerous benefits, AI possesses qualities that could pose threats in various applications, especially within the financial sector. Unlike algorithmic approaches that allow for the investigation of AI judgments, neural networks lack interpretability. Thus, when examining suspicious transactions, it becomes challenging to pinpoint the specific areas of the matrices responsible for detecting patterns like payment splits and consolidations. Thus, the algorithm's reliability can only be statistically tested by assigning it numerous tasks and evaluating its performance. There are several other issues, including:

- Hallucinations, where AI generates illogical results even with accurate data. There have been cases where AI fabricated legal precedents or offered non-existent discounts.
- Minefields, which occur when AI generates completely wrong results after a minor change to the initial data. This phenomenon is utterly incomprehensible, making it tough to combat.
- Overtraining, when an increase in the quantity and quality of input data inexplicably leads to a degradation in output quality.

And a number of others.

These challenges can be partially mitigated by employing multicomponent systems, where one neural network checks the output of another. However, there is no definitive solution to these challenges today.

ABUSE OF AI FOR ML/TF

Being a powerful tool, AI, naturally, piqued the interest of criminals. Although there is currently no classification of AI applications for money laundering or terrorist financing, potential cases include using bots to interact with banks during onboarding, creating fake identities, simulating identities through remote identification, optimizing scripts for social engineering, and optimizing illegal transaction graphs. This is a topic worthy of its own article.

There is no doubt that AI will find effective applications in the banking industry in general, and in AML/CFT in particular. However, the author believes that the practical capabilities of AI at its current developmental stage may be overstated and will undergo significant reassessment in the near future. Nevertheless, the analysis of AI capabilities and the development of a strategy to prevent illicit usage of AI should be prioritized by analysts and practitioners in the AML/CFT field.

ARTIFICIAL INTELLIGENCE IN FINANCIAL MONITORING

Artificial intelligence applications are now commonplace in almost every sphere of activity, with the banking industry often leading the charge in adopting innovative IT solutions and products

MIKHAIL PRONIN,
Vice President, Director of the Financial Monitoring Department, PSB Bank; Ph.D. in Economics

We see a lot of successful solutions in lending, transactional customer service, and especially in areas where expertise is heavily reliant on automated analysis of customer data and customer behavior.

The AML domain, with its focus on identifying suspicious client activity, presents a fitting arena for the integration of machine learning techniques, a subset of artificial intelligence.

The analytical function of PSB Bank's financial monitoring unit began experimenting with machine learning tools back in 2020, with a primary focus on developing various mathematical models for detecting irregularities in clients' payment behavior.

We were able to attain certain qualitative results by using an algorithm that combined a decision tree and logistic regression. However, significant success was achieved only after a considerable period, when this model surpassed the proficiency of experienced analysts.

Nonetheless, we received valuable insights that shaped the bank's future strategy.

First and foremost, we discovered an interesting pattern. In most circumstances, suspicious clients often mirror normal consumer behavior to evade detection.

Such mimicking of the typical conduct of bona fide consumers leads to the fact that mathematical models label some diligent clients that demonstrate aberrant behavior as suspicious instead of those that really have malevolent intents. Such specifics are common among young aspiring entrepreneurs or in niche business sectors. In that case, the unconventional payment behavior is justified by the unique nature of their business.

Secondly, the constant adjustment of high-risk clients' behavior to standard behavior causes continuous changes in the analytical data itself, as the evolving landscape renders previously effective models obsolete. Furthermore, the more closely we monitor this sector with machine learning technologies and complex analytical models, the faster it changes.

In this way, the use of artificial intelligence systems in financial monitoring differs significantly from their application in other domains. For example, in retail, the in-store consumer behavior model based on a large amount of data is quite accurate and consistent, making it is easy to predict consumers' behavior.

▲ **Panel discussion at the finals of the III International Olympiad on Financial Security**

After experimenting with incorporating artificial intelligence in financial monitoring, we discovered that while our team was well versed in the ML/TF risk analysis, they lacked expertise in machine learning tools. So, in 2022, we made the decision to recruit data analysts directly into our AML/CFT unit.

It is important to understand that a data analyst is fundamentally different from a client analyst who does anti-money laundering investigations. This is a completely separate field that necessitates personalized communication and specialized professional tools. As a result, our organization obtained data sandboxes, powerful computers, Python programming and BI data visualization tools.

Next, we established a partner environment in which client analysts could provide hypotheses about potential new approaches for recognizing suspicious consumers, and data analysts could convert such hypotheses into appropriate models. The resulting models were put into routine operation, and client analysts received findings obtained during such operation to validate them. If model efficiency dropped, client analysts developed a hypothesis to alter the model or an entirely new hypothesis for the same risk, which was then passed to data analysts via the aforementioned algorithm.

The creation of a shared communicative space for client analysts and data analysts resulted not only in synergistic joint work, but also in extensive reciprocal staff training and the development of new competencies. Data analysts became more competent in the subject area. Naturally, the purpose was not to transform them into client analysts, as we already have such people. However, joint work made them understand how the AML sphere works in terms of approaches to data management. As a result, data analysts learned how to choose the most appropriate data processing tools for various hypotheses.

Client analysts did not fall behind either. Prior to collaboration, they perceived information technology to be complex and out of reach. However, after seeing how it works, they took on some of the functions of data analysts. Besides, familiarity with

data analytics tools enabled client analysts to develop more advanced risk identification hypotheses.

Overall, this is a fascinating experience that we refer to as a natural-artificial intelligence cooperation.

We extended this cycle to other activities, thus ensuring:

1. Quick response to new risks and suspicious client activity patterns provided by the Bank of Russia and Rosfinmonitoring. The trial setup of new risk models takes no longer than two banking days.

2. Continuous enhancement in the effectiveness of analytical rules used for monitoring client activities online and offline. As a result, despite an ever-increasing number of customers, we do not need to enlarge our workforce.

3. Capability to test a huge number of our own hypotheses for detecting new sorts and enhanced versions of classic suspicious transaction schemes. Every quarter, at least ten hypotheses turn from an idea into a functional algorithm.

Here is another fascinating observation. In October 2023, as part of the Rosfinmonitoring Olympiad on Financial Security, we held a workshop for students, where we discussed our analytical project Patterns. This is an internal project that aims to create a new, extremely effective tool for detecting suspicious customer transactions.

In fact, the opportunity to implement this project arose thanks to the accumulated machine learning experience with the participation of data analysts, as well as our client analysts' new skills in creating analytical hypotheses.

When we shared our impressions of successful symbiosis with the students and daydreamed about how amazing it would be if future specialists could combine all of these skills: analyze clients, generate hypotheses, as well as program and apply them to identify high-risk operations, students were surprised that this was not yet the case. Can you believe it? Our present students, who are taking part in the Rosfinmonitoring Olympiad on Financial Security, hope to become such specialists. Not only do they have this vision, but they also actively prepare for this type of work by acquiring knowledge and skills.

With such a motivated youthful generation, we are confident that the future of anti-money laundering will be bright. A future in which both natural and artificial intelligences will efficiently interact and evolve.

"AFTER EXPERIMENTING WITH INCORPORATING ARTIFICIAL INTELLIGENCE IN FINANCIAL MONITORING, WE DISCOVERED THAT WHILE OUR TEAM WAS WELL VERSED IN THE ML/TF RISK ANALYSIS, THEY LACKED EXPERTISE IN MACHINE LEARNING TOOLS. SO, IN 2022, WE MADE THE DECISION TO RECRUIT DATA ANALYSTS DIRECTLY INTO OUR AML/CFT UNIT"

ALEXEI GELETA:

"RUSSIA'S FINTECH MARKET STANDS OUT AS ONE OF THE MOST INNOVATIVE AND ADVANCED IN THE WORLD"

Prior to implementation, fintech initiatives undergo an independent expert review, evaluating potential risks and threats, as well as their impact on citizens, the state, and businesses. Managing this expert review is the Digital Compliance Group of the Analytical Center under the Government of the Russian Federation. We discussed the group's activities and the current impact of financial awareness with Alexei Geleta, the group's head

1. The Federal Financial Monitoring Service collaborates closely with the Analytical Center under the Government of the Russian Federation on various projects, including those executed jointly with the Digital Compliance Group, which you lead. Could you elaborate on the Group's tasks and share your personal experiences in this field?

In 2020, the Analytical Center under the Government of the Russian Federation established a new area of expertise in the public sector — digital compliance. Its core functions include interagency coordination of fintech initiatives and the provision of comprehensive, independent analytical and regulatory expert reviews, drawing from international experience. Our work spans risk and threat identification and the development of the fintech market, tailored to meet the needs of the government, businesses, and citizens.

My understanding of compliance systems began during my academic years. Graduating from the profile department of the MEPhI Financial and Economic Security Institute, which received support from the Federal Financial Monitoring Service, provided me with both theoretical knowledge and practical skills, including during my internship at the agency. Subsequently, working in the banking sector allowed me to gain fundamental and versatile compliance experience. I was actively involved in building and automating compliance risk management systems at the parent bank level, as well as coordinating Russian and foreign financial organizations within the group concerning AML/CFT and compliance risks. The objective was to ensure compliance with the bank's uniform standards and local regulations.

2. What are the core activities of the Digital Compliance Group at the moment?

The Digital Compliance Group is primarily focused on three key areas:

1. Addressing "grey" areas that necessitate comprehensive expertise and recommendations for further management decisions at both federal and regional levels. These areas encompass crypto mining and digital currency turnover, demanding a deep understanding of projects initiated by business entities involved in automated systems, blockchain technologies, and payment mechanisms.

2. Identifying risks and threats to the national financial system and socio-economic area. We develop procedures to identify illicit banking transactions (such as mis-selling), fraud disguised as welfare payments, cashback payments, and fraudulent resources in the COVID-19 crisis, to name a few. While delving into the specifics of our work process and results is unnecessary, it's imperative to comprehend the underlying causes of threats, structure customer journeys and business processes, pinpoint the most vulnerable areas, establish data flows, build analytical dashboards, engage in interagency collaboration, and draft analytical reports with recommendations to mitigate or eliminate identified threats.

3. Facilitating the development of payment mechanisms. Despite attempts of external pressure, Russia's fintech market stands out as one of the most innovative and advanced in the world. However, there are areas for growth, necessitating the updating of conservative approaches or the establishment of a new regulatory framework for financial system development. Addressing these challenges requires ongoing communication and mutual understanding between business representatives, who propose new ideas for national financial system development, and agencies responsible for ensuring financial system security within their scope of authority. The Coordination Center of the Government of the Russian Federation aids in fostering understanding devoid of excessive bureaucracy, facilitating significant progress in addressing pressing issues.

3. In your opinion, which processes in fintech are conservative?

Identification of individuals, especially when opening a bank account. We see successful digitization of processes in various socio-economic areas. While various socio-economic areas have seen successful digitization of processes, facilitating faster and easier management of everyday and business matters, opening a bank account remains an exception.

Nevertheless, progress has been made in this regard. Responding to requests from banking sector participants, the Coordination Center, in collaboration with the Bank of Russia, the Federal Financial Monitoring Service, and other relevant agencies, initiated the development of remote identification tools for foreign citizens opening bank accounts with Russian credit institutions, a project commonly referred to as the "Tourist Card." Through coordinated efforts, relevant amendments to national anti-money laundering legislation were introduced. Foreign citizens meeting specific criteria and conditions can now remotely open bank accounts with Russian banking organizations, receive virtual MIR cards, and utilize them before arriving in Russia. However, feedback from credit organizations highlights emerging challenges necessitating collaborative solutions.

The regulation of crypto mining and cryptocurrency turnover has also been a contentious issue for years. While all agencies recognize the risks and threats associated with cryptocurrencies, consensus on how to address them remains elusive. Two opposing views prevail: some advocate for banning cryptocurrency circulation involving the Russian financial system to mitigate risks and threats, while others argue for the establishment of clear regulatory frameworks for all participants in the Russian crypto market. At the expert level and considering the growing interest* of citizens in cryptocurrencies, I am inclined towards a risk-based regulation of the crypto market, allowing for the distinction between diligent and non-diligent participants. While banning may seem like the simplest solution, it raises questions about enforcement and compliance for authorities and credit organizations, potentially resulting in fines and ineffective regulations.

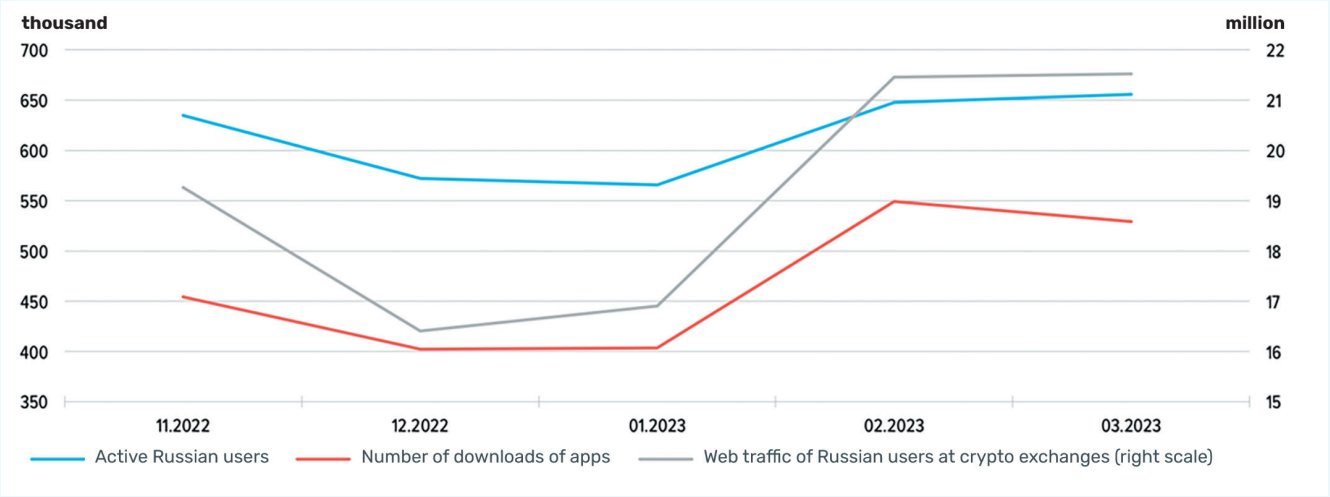
4. Do you believe that new technologies can enhance the protection of financial services users from scammers? Or rather, it's yet another tool for criminals?

It's a paradox: new technologies can both enhance security and serve as a tool for criminals. Indeed, fraudsters often leverage new technologies much faster than authorities can adapt to them. Consider the cases of fraud utilizing deepfake and voice spoofing technologies — this trend is likely to continue growing.

5. What is the role of financial awareness in the context of digitization: did the Analytical Center conduct case studies?

The numbers paint a concerning picture: losses from fraud involving digital services among the population are escalating annually. According to the Bank of Russia, cyber fraudsters

Russian users' activity on cryptocurrency exchanges



Source: https://www.cbr.ru/Collection/Collection/File/44007/4q_2022_1q_2023.pdf

stole RUB 15.8 billion from Russians in 2023, as evidenced[1] by the review of unauthorized transactions — a staggering 11.48% increase from 2022.

Various agencies in Russia have developed extensive knowledge bases to enhance financial awareness. The Federal Financial Monitoring Service, for instance, has successfully conducted the International Olympiad on Financial Security, accumulating a wealth of experience and practical cases beneficial for the population amidst rapid digitization. Educational initiatives, ranging from online games to quizzes and other digital learning formats, hold promise for implementation in educational, governmental, corporate, and other institutional settings.

6. Digital compliance in Russia: are there any unique features?

Regarding digital compliance within Russian banks, it would be best to consult with them directly or discuss it at the Compliance Council hosted by the Federal Financial Monitoring Service — a forum in which I would gladly participate!

As for the department I lead, the Digital Compliance Group, it operates within the Coordination Center of the Government of the Russian Federation, serving as an independent expert hub for governmental managerial decisions.

"THE REGULATION OF CRYPTO MINING AND CRYPTOCURRENCY TURNOVER HAS ALSO BEEN A CONTENTIOUS ISSUE FOR YEARS. WHILE ALL AGENCIES RECOGNIZE THE RISKS AND THREATS ASSOCIATED WITH CRYPTOCURRENCIES, CONSENSUS ON HOW TO ADDRESS THEM REMAINS ELUSIVE"

[1] https://www.cbr.ru/press/event/?id=18419

IDENTIFYING AND COMBATING CYBERCRIME

COUNTERING "MONEY MULES" AND HIGH-RISK P2P TRANSACTIONS IS A PRIORITY VECTOR OF FINANCIAL MONITORING

The Bank of Russia observes an increase in risks associated with individuals using the Russian banking sector for P2P transactions to secure settlements for shadow businesses. These concerns are directly linked to so-called money mules — people whose accounts are used for such illicit P2P transfers. The Bank of Russia is working closely with banks to develop and implement strategies to counter such operations, including efforts to improve the efficiency of identifying mule accounts and responding to recognized threats

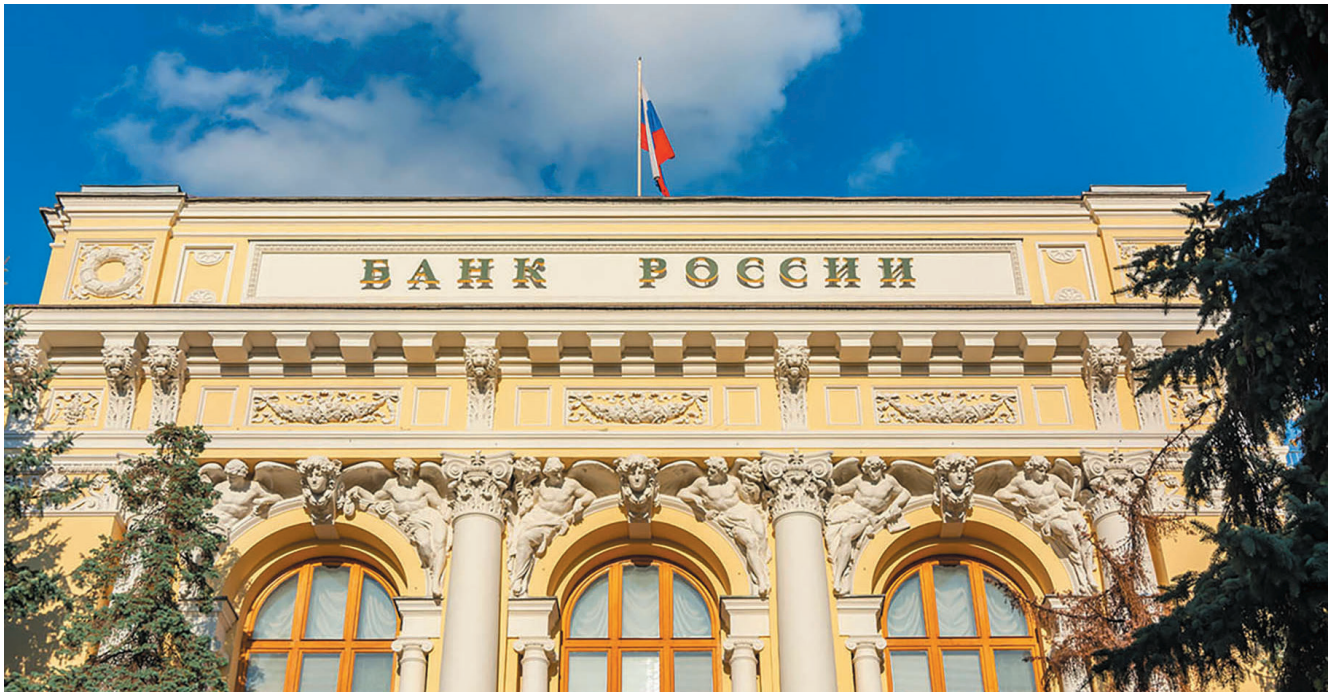
BOGDAN SHABLYA,
Director of the Financial Monitoring and Currency Control Department, Bank of Russia

Supervision and monitoring of credit institution operations indicate that unscrupulous entities are using credit institution P2P services for high-risk transactions. Such transactions enable shadow enterprises, which do not have access to formal financial services, to receive funds. Underground businesses include online casinos and bookmakers, financial pyramids, content pirates that violate copyrights, various fraudulent websites, illegal product dealers, cryptocurrency exchanges, and P2P crypto services that use money mules.

Citizens involved in such operations risk not only losing their savings to numerous fraudulent schemes, but also engaging in illicit activities that may incur criminal liability. Given the enormous volume of transactions by such shadow enterprises, banks may encounter situations that jeopardize the interests of their creditors and depositors.

In 2020-2022, such transactions were conducted via acquiring services, with a focus on small credit institutions that specialize in providing shadow banking services. Transfers were predominantly executed utilizing the accounts of international payment service providers, legal entities, enterprises established specifically for this purpose, and unscrupulous financial organizations conducting illegal activities under the guise of microloans and similar ventures.

Throughout this period, the Bank of Russia worked to eliminate high-risk transactions and financial institutions that were routinely involved in such transactions from the banking system.



THE LAUNCH OF THE KNOW YOUR CUSTOMER PLATFORM

made it considerably more difficult to conduct such transactions using the accounts of legal entities and entrepreneurs. The withdrawal of international payment systems, which had previously facilitated high-risk activities through foreign acquiring banks, caused significant changes in the shadow payment sector.

As a result, in 2023, high-risk transactions transitioned into direct P2P settlements via payment cards and money mule accounts who either open an account or have a bank card issued in their name and then transfer them to the disposal of shadow business participants. Examples of P2P transactions include card-to-card and wallet-to-wallet money transfers, as well as transfers from the account of a telecom provider's subscriber to a wallet/card and back.

The volume of high-risk P2P operations in the banking sector, along with the number of money mules involved in their execution, is currently estimated to be high, necessitating a thorough response. The management of the Bank of Russia underscores the importance of prioritizing efforts in this area.

On the one hand, our estimates indicate that using P2P settlement mechanisms for shadow business proves to be more complex and costly than acquiring operations. One of the reasons for this is the need to maintain an IT infrastructure to automate and manage transactions across various mule accounts. On the other hand, a number of factors contributed to the transition to the P2P scheme, including:

- Bank cards and e-wallets offer simplicity and accessibility, facilitating large-scale P2P operations with minimal restrictions and fees. While these banking products are convenient for the general public and companies, shadow banking entities exploit this accessibility. For instance, money mule managers recruit citizens, often unknowingly, to hand over newly created accounts/wallets to unauthorized individuals. Subsequently, dozens of virtual cards are linked to the account, through which large sums of money are processed within days.

- The identification process for individuals when opening e-wallets can be conducted through third-party organizations, such as payment agents and telecom operators, which may have less stringent identity verification measures due to their income being based on the number of e-wallets opened. Existing legislation permits the utilization of public information systems for simplified identification during e-wallet opening, without requiring personal presence or original copies of ID documents. Instances have been identified where credit institutions constructed e-wallets using individuals' personal information without their consent, leading to significant risks for residents.

- Some publicly available online P2P services provided by credit institutions exhibit technical vulnerabilities. Shadow businesses exploit fictitious P2P payment forms on their websites to gather credit card information and automatically redirect it to credit institutions' real websites to complete a P2P transaction.

To mitigate these risks, the Bank of Russia published Guidelines No. 16-MR[1] dated September 6, 2021 and No. 13-MR[2] dated October 12, 2023.

Guidelines No. 16-MR mandate that credit institutions identify suspicious money transfers between individuals using electronic payment methods, such as payment cards and e-wallets. They are also required to implement anti-money laundering measures and secure their P2P services.

To reduce the risks associated with using acquiring services to bypass Guidelines No. 16-MR, the Bank of Russia introduced Guidelines No. 13-MR, advising acquiring credit institutions to ensure that funds are credited to the accounts of the enterprise where the purchase was made to prevent tax fraud schemes. Additionally, they are urged to monitor indicators of unusual transfers to enterprises that do not engage in legitimate business activities.

We are now collaborating closely with banks to develop and introduce innovative solutions to counter high-risk P2P transactions. Such solutions also help in identifying accounts and transactions involving money mules, including in real time, as well as introduce additional verification procedures for issuing bank cards and utilizing particular banking products.

The main objective is to complicate shadow business activities and render the utilization of the banking industry and P2P operations for shadow companies as challenging and costly as possible.

Additionally, we aim to foster a zero-tolerance stance on money mules among financial institutions and the public. This entails developing compliance procedures to prevent the servicing of drop accounts, as well as conducting collaborative awareness-raising initiatives involving the Bank of Russia, credit institutions and law enforcement agencies to educate the public about the repercussions of such activities and cultivate a negative perception towards them.

"WE ARE NOW COLLABORATING CLOSELY WITH BANKS TO DEVELOP AND INTRODUCE INNOVATIVE SOLUTIONS TO COUNTER HIGH-RISK P2P TRANSACTIONS. SUCH SOLUTIONS ALSO HELP IN IDENTIFYING ACCOUNTS AND TRANSACTIONS INVOLVING MONEY MULES, INCLUDING IN REAL TIME, AS WELL AS INTRODUCE ADDITIONAL VERIFICATION PROCEDURES FOR ISSUING BANK CARDS AND UTILIZING PARTICULAR BANKING PRODUCTS"

[1] On credit institutions' growing attention to some transactions of individual clients.
[2] On credit institutions' and payment aggregators' activities related to transactions carried out using E-payment methods.

INFORMATION SECURITY IN FINANCIAL MARKET: COUNTERING CYBER FRAUD IN MONEY TRANSFERS

The widespread adoption of digital payment technology has fundamentally transformed society's approach toward information security. With the rapid expansion of remote banking services, the absence of adequate measures to safeguard bank customers from cyber fraud can have profound societal repercussions[1]. Therefore, today, the capacity to effectively mitigate the risks of fund theft from citizens' accounts is one of the most important issues in defending the rights of financial service users and increasing trust in digital technologies

VADIM UVAROV,
Director of the Information Security Department, Bank of Russia

Countering cyber fraud in the credit and financial sectors is one of the Bank of Russia's priorities. Through collaborative efforts with industry stakeholders, the regulator's methodical endeavors revealed that banks thwarted approximately 34.8 million fraudulent transaction attempts in 2023, preventing the theft of RUB 5.8 trillion from credit institutions' customers.

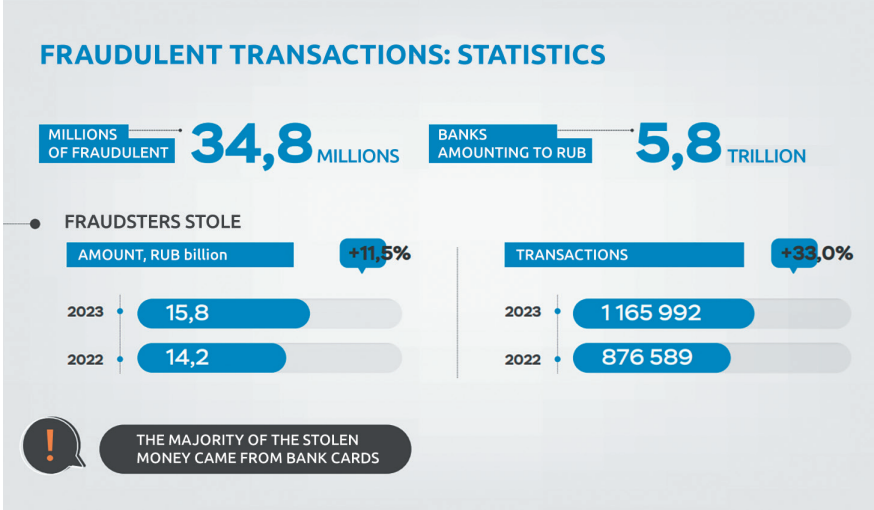
However, despite these efforts, the Bank of Russia has observed a consistent annual rise in unauthorized transactions completed without the consent of bank customers. In 2023, cybercriminals managed to steal RUB 15.8 billion, marking an 11.5% year-over-year increase. The number of fraudulent transactions surged by 33% to over 1.1 million cases[2].

One of the problems preventing a significant shift in the situation with fraud and social engineering is continuous evolution of schemes and tactics by fraudsters. Currently, there is a tendency toward tailored attacks, in which offenders thoroughly investigate the personal information of possible victims, including their data uploaded on various web resources.

In response, the Bank of Russia takes a comprehensive approach to combating telephone and Internet fraud. The set of measures includes improvements to legislation governing financial organizations' activities, outreach to citizens, and collaboration with law enforcement and supervisory authorities, domain name registrars, and telecom operators.

[1] According to official data from the Russian Ministry of Internal Affairs, information and telecommunications technology was used to commit every third crime in the country in 2023. During that year, there was a 29.7% increase in registered criminal offenses within this sector compared to 2022 (https://mvdmedia.ru/news/official/statisticheskie-svedeniya-o-sostoyanii-prestupnosti-v-2023-godu/).

[2] The Bank of Russia publishes annual reports on transactions made without the authorization of financial institution customers on its official website (http://www.cbr.ru/analytics/ib/operations_survey/2023/).



In July 2024, a new law on enhancing the methods for combating the theft of bank customers' funds, developed with the involvement of the Bank of Russia, will go into effect[3]. The law mandates banks to:

- Introduce a two-day cooling-off period, requiring the bank to suspend money transfers to banking details included in the Bank of Russia's database of instances involving attempts to transfer money without the client's authorization (hereinafter referred to as the "Bank of Russia's Database"). During this two-day period, customers have the opportunity to reconsider their actions and reverse the transfer of funds to suspicious accounts.

- Disable access to electronic payment methods for money mules if information about their illicit behavior is provided by the Russian Ministry of Internal Affairs and entered into the Bank of Russia's Database. However, if a financial organization reports such information, the bank may choose to disable access at its discretion.

- Reimburse the client within 30 days if the bank permitted funds to be transferred to a fraudulent account included in the Bank of Russia's Database, failing to perform the mandatory customer protection procedures.

A public survey conducted by the Bank of Russia in 2023 on the satisfaction level with the security of financial services revealed that over 62% of citizens who fell victim to fraud reported it to the bank and/or the police. Streamlining information flow between banks and law enforcement agencies is crucial for combating fraudulent transactions.

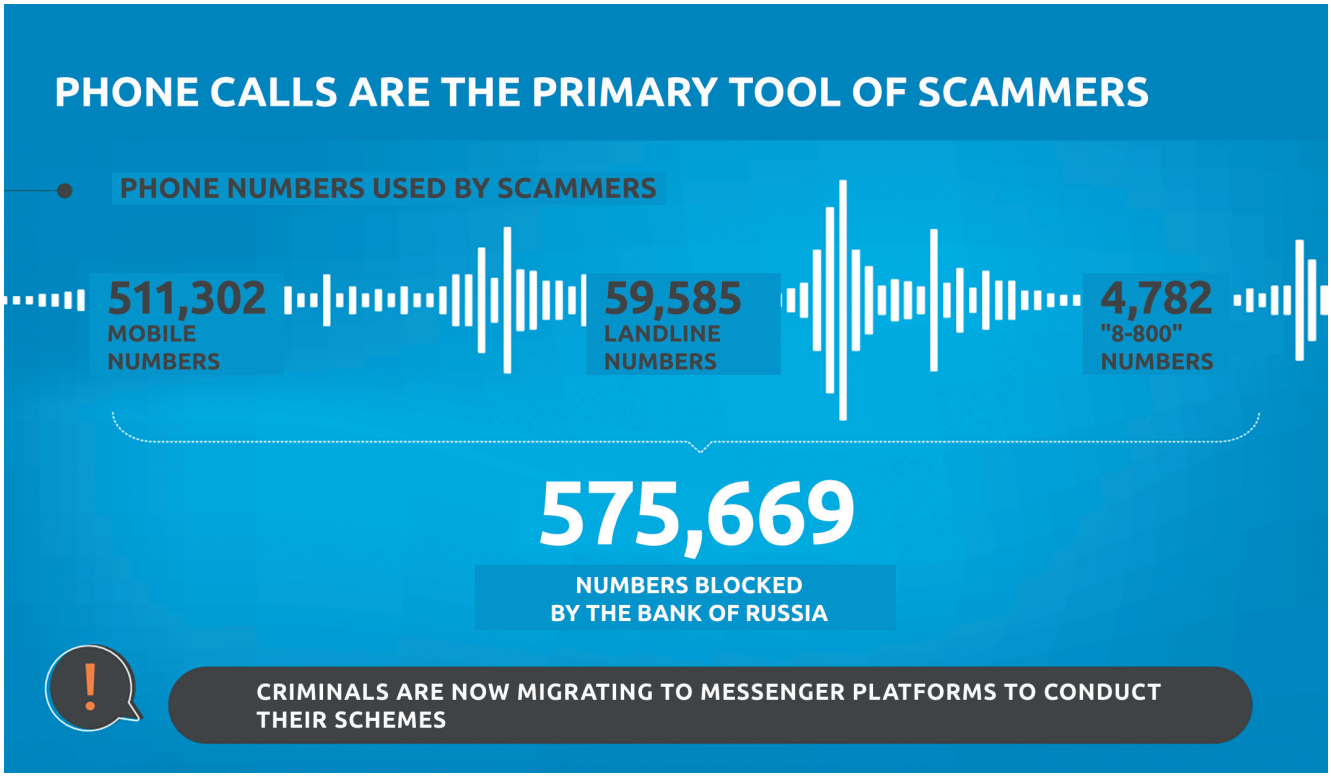
In October 2023, the law on information exchange between the Bank of Russia and the Ministry of Internal Affairs of Russia went into effect[4], enabling automated transmission of data on unauthorized transactions between these agencies. Law enforcement agencies can now promptly access information required for investigating fraud and criminal cases from the Bank of Russia's Database. Banks, in turn, can use the information received from the Ministry of Internal Affairs of Russia in their anti-fraud systems to prevent further fraudulent transactions.

To combat illicit online activity, the Bank of Russia collaborates with the General Prosecutor's Office of the Russian Federation[5] and domain name registrars. In 2023, the regulator identified and reported over 38,300 websites that had been misused for illegal activities and ordered their blocking. The majority (55%) of these resources were phishing sites

[3] Federal Law on Amendments to Federal Law on the National Payment System No. 369-FZ dated July 24, 2023.

[4] Federal Law on Amendments to Article 26 of Federal Law on Banks and Banking and Article 27 of Federal Law the National Payment System No. 408-FZ dated October 20, 2023.

[5] Within the powers provided for in Article 6.2 of Federal Law on the Central Bank of the Russian Federation (Bank of Russia) No. 86-FZ dated July 10, 2002.



designed to obtain financial institution customers' data. Additionally, the regulator requested access restrictions to 4,500 social network groups and 35 applications used by perpetrators for illicit activities and phishing under the guise of operating credit institutions.

The Bank of Russia requested to blacklist 575,700 phone numbers used by scammers to steal funds from individuals.

The monitoring conducted by the Bank of Russia this year highlighted two key negative social trends: the increase in credit fraud and the involvement of individuals, particularly young people, in money muling.

Credit fraud poses significant challenges, not only due to the rising average theft amounts but also because people, who take out loans under the influence of perpetrators and transfer the borrowed funds to them, fall into long-term debt traps. The Bank of Russia is developing measures to protect Russian residents and strengthen the accountability of credit institutions. These include the cooling-off period between loan approval and fund transfer to the borrower. This approach should first and foremost apply to large loans. It is similarly crucial to incorporate anti-fraud processes into the loan pipeline to help banks identify borrowers acting under the influence of third parties.

In addition, the Bank of Russia is actively combating money muling, which involves the cashing-out of illegally obtained funds by money mules, including via electronic payment options. Individuals can participate in money muling in a variety of ways. In some cases, they participate intentionally, but are not necessarily aware of the potential consequences for themselves. In other circumstances, people are unaware that they are involved in criminal activities. People might unintentionally become accomplices in money muling by exposing personal information in the public domain, such as on social media. The most vulnerable age groups are adolescents and young people (the majority of money mules are between the ages of 17 and 19).

To address this issue, in April 2022, the Bank of Russia advised credit institutions to disable electronic payments for individuals whose payment cards are used to withdraw and cash out stolen funds[6]. As a result, banks now have the authority to suspend online account management access when a client engages in suspicious activity.

The aforementioned law on enhancing the methods for combating the theft of bank customers' funds, effective from July 2024, will introduce

[6] Information Letter of the Bank of Russia on Measures to be Taken by Credit Institutions to Prevent Money Transfers without Customer Authorization No. 01-56-5/3143 dated April 15, 2022.

stricter rules for restricting remote banking services for money mules. Banks will be required to suspend a client's access to electronic payment methods if information about their illicit behavior is provided by the Russian Ministry of Internal Affairs and entered into the Bank of Russia's Database. Since this information is shared with all credit institutions, remote operations on money mules' accounts will be halted across all banks.

This policy will render such illicit operations economically unprofitable for criminals.

To enhance communication between credit institutions and customers, the Bank of Russia developed Recommendations and had them approved by the Russian Ministry of Internal Affairs[7]. These recommendations promote customer awareness measures to combat money muling. The primary objectives of these awareness campaigns are to educate citizens about the responsibility and consequences of participating in money muling, as well as to highlight its illegality and unfavorable image.

The banking industry's efforts to combat various forms of cyber fraud, including credit fraud and money muling, heavily rely on the quality of data on suspicious transactions submitted by banks to the Bank of Russia's Database. The regulator then disseminates this information to all participants in the information exchange. The accuracy, reliability, and timeliness of this information are crucial for the effectiveness and speed of combating criminals, as well as for the quality of anti-fraud systems in banks. Therefore, ensuring adequate data reporting to the Bank of Russia is now one of the regulator's top priorities, including in its supervisory activities. This is essential to ensure that the systems in place to combat fund theft under applicable laws protect the rights and interests of financial service consumers.

[7] Methodological Recommendations on strengthening customer awareness by credit institutions to prevent unauthorized transfers of funds, loan contracts influenced by fraud or abuse of trust, transactions with such funds, and citizen involvement in the cashing-out of proceeds of crime No. 3-MR dated February 28, 2024.

PRE-TRIAL RESTRICTION OF ACCESS TO INFORMATION ON THE INTERNET, THE DISTRIBUTION OF WHICH IS PROHIBITED ON THE TERRITORY OF THE RUSSIAN FEDERATION

In recent years, one of the most pressing issues has been the use of information and communication technology (ICT) in criminal activities, which poses a severe threat to the Russian Federation's national security

ANTON RASTASHCHENOV,
Head of the department for preventing the spread and identifying destructive and prohibited information on the Internet
Directorate for organizing the fight against illegal use of information and communication technologies of the Ministry of Internal Affairs of Russia
Lieutenant Colonel of Police

Rapid advancements in information technology have enabled criminals to evade detection by law enforcement agencies, leading to a surge in cybercrimes.

Official data indicates that there were 677,000 offenses involving ICT documented by internal affairs authorities between January and December 2023, representing a 29.7% increase compared to the previous year.

This upward trend underscores the urgency of identifying effective strategies and methods for detecting, preventing, suppressing, disclosing, and investigating cybercrimes.

Preventive measures aimed at countering illegal information resources used by criminals for advertising/propaganda, money laundering, and crime financing platforms are critical components of combating cybercrime.

Under current legislation, the Russian Ministry of Internal Affairs collaborates with Roskomnadzor to block access to web resources containing prohibited content, including information related to drugs, weapons, and harmful extremist ideologies.

In 2023, the diligent efforts of these agencies led to the restriction of access to over 330,000 websites and pages hosting prohibited content.

Such prohibited content typically originates from specially designed web resources, such as specialized websites and forum pages, as well as social media groups. Additionally, those involved in creating these illicit platforms may operate from outside Russia and employ various technologies and resources to maintain their operations.

The rights and regulations concerning the search, acquisition, transfer, generation, and distribution of information, as well as information technology application and information security, are governed by Federal Law No. 149-FZ dated July 27, 2006[1].

[1] Federal Law on Information, Information Technologies and Information Protection No. 149-FZ dated July 27, 2006 (hereinafter the "Federal Law No. 149-FZ").

Article 15.1 of the Federal Law No. 149-FZ, effective November 1, 2012, governs the mechanism for blocking web resources. This mechanism comprises a set of organizational and technical measures aimed at restricting access to banned content distributed on the Internet.

As a rule, dissemination sources of prohibited information are specially created Internet resources, which are specialized websites and forum pages, as well as thematic groups on social networks. Meanwhile, persons engaged in creating aforementioned platforms may be located abroad, using tools and resources for moderation.

Part 2 of Article 15.1 of the Federal Law No. 149-FZ states that the Uniform Automated Information System of the Russian Internet Blacklist[2] should include domain names, website references, and network addresses facilitate the identification of websites containing information the distribution of which is prohibited in the Russian Federation.

According to Part 5 of Article 15.1 of the Federal Law No. 149-FZ, a web resource may be added to the Russian Internet Blacklist based on decisions made by executive federal bodies authorized by the Russian Federation's Government. These decisions must be duly approved in accordance with the Government's procedure[3] and may also require a court ruling recognizing the distributed information as prohibited in the Russian Federation.

Subparagraphs a) to l) of Article 15.1, Part 5, Paragraph 1 of the Federal Law No. 149-FZ provide a comprehensive list of prohibited information. The federal executive bodies authorized by the Russian Federation's Government use the list to make decisions within their competence.

Subparagraphs b) and j) of Article 15.1, Part 5, Paragraph 1 of the Federal Law No. 149-FZ, in particular, mandate the inclusion of web resources in the Russian Internet Blacklist that publish the following information:

- Techniques for developing, manufacturing, and using narcotic drugs, psychotropic substances, and their precursors, as well as locations for acquiring such drugs, substances, and precursors, and ways and locations for growing narcotic plants;
- Methods for producing improvised explosives and explosive devices; illegal manufacturing or modification of weapons and major components of firearms; and unlawful production of ammunition, excluding information on how to make cartridges for civilian long-barreled firearms.

According to the National Security Strategy of the Russian Federation, approved by Decree of the President of the Russian Federation No. 683 dated December 31, 2015, one of the main threats to state and public security is the use of information and communication technologies for propagating ideologies such as fascism, extremism, terrorism, and separatism.

One of the most important aspects of information security in this regard is preventing the dissemination of extremist ideology, xenophobia, and ideas of national exclusivity via digital technologies.

Federal Laws No. 398-FZ dated December 28, 2013[4] and No. 327-FZ dated November 25, 2017[5] supplement the Federal Law No. 149-FZ with Article 15.3, which regulates the procedure for restricting access to content found in information and telecommunication networks, including the Internet, that contains calls for mass riots, extremist activities, and participation in mass (public) events held in violation of established procedure. It also covers information materials of foreign and international non-governmental organizations whose activities are deemed undesirable within the Russian Federation, as well as information providing access to such content.

Article 15.3, Part 1 of the Federal Law No. 149-FZ grants the General Prosecutor of the Russian Federation and his/her deputies the authority to request Roskomnadzor to limit access to information resources that disseminate the aforementioned content. This request can be triggered by reports from federal or regional authorities, local governments, organizations, or citizens regarding the distribution of such content in information and telecommunication networks, including the Internet.

[2] Hereinafter, the "Russian Internet Blacklist."

[3] Decree of the Government of the Russian Federation on the Uniform Automated Information System of the Russian Internet Blacklist No. 1101 dated October 26, 2012 (hereinafter, the "Decree No. 1101").

[4] On Amending Federal Law on Information, Information Technologies, and Information Protection.

[5] Information, Information Technologies, and Information Protection and Article 6 of the Law of the Russian Federation on Mass Media.

Upon receiving a request from the Russian Federation's General Prosecutor or one of his/her deputies, Roskomnadzor promptly notifies telecom providers to impose access restrictions on the information resource or its contents. The operator is then required to immediately block access to the specified information resource. Additionally, Roskomnadzor adds information on such web resource to a dedicated database.

The procedure enables rapid response to incidents involving the circulation of such prohibited content on the Internet. Besides, Roskomnadzor's request must include details such as the website's domain name, network address, and page references to identify information, further enhancing the effectiveness of the procedure.

CURRENT TRENDS IN THE MARKET OF ILLEGAL FINANCIAL SERVICE PROVIDERS

Ensuring the safety of people's incomes and protecting consumers from involvement in illicit activities in the financial market are among the foremost priorities of financial regulators

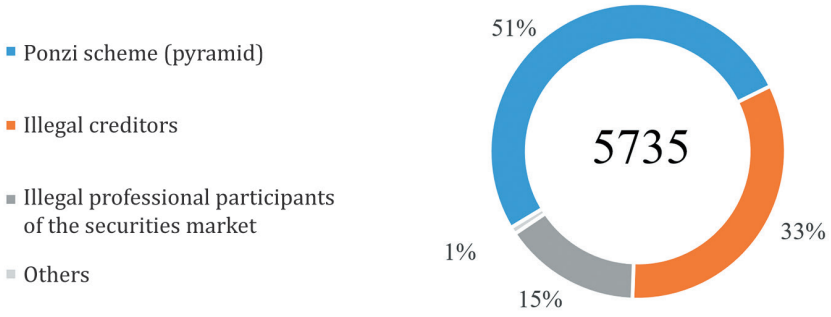
ROMAN MUKHLYNOV,
Deputy Director of Non-Bank Credit Department, Central Bank of the Russian Federation

The Bank of Russia is taking steps to consolidate the efforts of all stakeholders in order to protect citizens' savings from scammers and to counter unfair and illegal practices.

In 2023, the Bank of Russia identified 5,735 entities (companies, projects, individual entrepreneurs and others) exhibiting signs of illicit activity, including signs of Ponzi schemes (financial pyramids). The number represents a 15.5% increase from the previous year, although, the life cycle of such projects decreased, as did the average transaction amount. Information on all identified cases is forwarded to law enforcement agencies, the Federal Financial Monitoring Service, Federal Antimonopoly Service of Russia, and the Federal Service for Supervision of Communications, Information Technology, and Mass Media — to combat fraudulent activities. However, scammers use new schemes and tools each year, therefore, particular caution is required in detecting such practices, both on the part of the regulators, law enforcement, the public, and financial organizations.

The landscape of financial crime has undergone notable shifts in recent years, with a significant move towards online engagement and the utilization of cryptocurrency by both fraudsters and illicit financial entities. The Bank of Russia has consistently underscored the risks associated with the proliferation of cryptocurrencies within the Russian

▸ **Distribution of entities engaged in illegal activities in 2023**



Federation, citing threats to both public welfare and the stability of the financial system. These risks include potential involvement of financial institution clients in unlawful activities such as money laundering and terrorist financing[1]. In response, recommendations have been formulated to mitigate these risks for clients of banks and other financial entities[2].

Equally risky is the growing number of illegal financial market participants who attract investments in cryptocurrency. In 2022, every other pseudo investment project involved cryptocurrency; in 2023, almost all pyramids and unauthorized FX clubs offered investments in internal tokens or accepted contributions in cryptocurrency.

The use of cryptocurrencies in criminal activities poses high risks explained by the difficult tracking of cryptocurrency transactions, thereby complicating efforts to identify the ultimate beneficiaries of criminal schemes. Criminals quickly adapt to evolving circumstances, making it increasingly difficult to withdraw funds from fraudulent cryptocurrency projects. Among the 2,944 pyramid schemes identified in 2023, more than 45% offered "investors" to use foreign payment service providers to transfer funds. Almost 1,500 scams accepted payments in cryptocurrency, which, among other things, allows the organizers and beneficiaries of the schemes to remain anonymous.

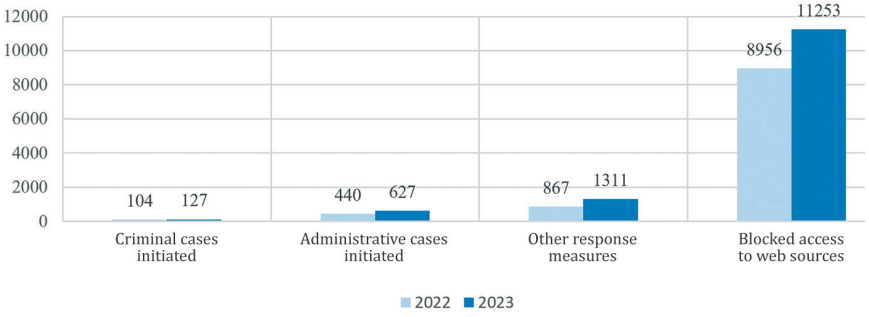
Amidst the steady increase in consumer interest in remote financial services and the growing reliance on information disseminated through social media, most financial pyramid schemes, pseudo-brokers, and even illegal creditors operate online. Consequently, an expanding number of consumers may find themselves vulnerable to fraudulent practices.

Recognizing this challenge, the Bank of Russia remains steadfast in its efforts to enhance the monitoring system of the information space. In the past year, the system saw the incorporation of automated content assessment, while the preceding year witnessed an expansion to include social networks and messaging platforms. These enhancements have bolstered the system's capacity to swiftly identify unauthorized providers of financial services.

Despite proactive measures such as blocking illegal sources at the Bank of Russia's initiative, fraudsters persistently adapt, often establishing similar websites with replicated content once their primary sites have been shut down. To fortify the efficacy of blocking efforts, the Bank of Russia introduced measures in 2023 enabling the simultaneous restriction of access not only to primary domains but also to all subdomains associated with illicit entities.

In 2023, following the initiative of the Bank of Russia, access to over 11,200 online sources was restricted, including accounts on popular platforms such as VKontakte, Odnoklassniki, and Telegram, which included more than 3,000 accounts, channels, and chatbots utilized by illegal financial market participants and financial pyramids. The total audience affected by these blocked resources exceeds 230 million users.

▸ **Bank of russia-initiated measures against illegal entities and financial pyramids**



[1] Information on risks and threats associated with the spread of crypto-assets (virtual currencies, cryptocurrencies) is available on the official website of the Bank of Russia on the Internet (press release on the Use of Virtual Currencies, Namely Bitcoin, in Transactions dated January 27, 2014; press release on the Use of Private Virtual Currencies (Cryptocurrencies) dated September 4, 2017; Report for Public Consultations Cryptocurrencies: Trends, Risks, Measures dated January 20, 2022).

[2] Information Letter of the Bank of Russia on the risks of transactions with digital currencies and recommendations to financial organizations to avoid offering services involving such transactions dated February 29, 2024 No. ИН-08-12/18.

Furthermore, since 2022, the Know Your Customer platform has been augmented with information on criminal entities, including companies and individual entrepreneurs. This integration enables banks to promptly access such data when evaluating the risk associated with their clients and their counterparts. It also facilitates the implementation of anti-money laundering measures against illegal financial service providers. Presently, the platform houses information pertaining to approximately 2,300 entities, encompassing pyramids, illegal creditors, forex FX clubs, among others.

In 2023, the Bank of Russia issued recommendations[3] for credit organizations to apply anti-money laundering measures based on reasonable grounds. This includes restricting account transactions of any company flagged for exhibiting signs of illegal activity, as published on the official website of the Bank of Russia, and their intermediaries. Such measures aim to curtail the lifespan of financial pyramids, hinder the accumulation of funds by illegal financial service providers, and mitigate losses incurred by the populace in criminal schemes.

For example, in the microfinance market, there is a heightened demand for online loans, with 75% of loan agreements with micro-finance institution (MFIs), up from 66% in 2022, being executed online. Hence, the number of cases where fraudsters impersonate borrowers to obtain loans from MFI and subsequently default on repayments have surged. These schemes harm two parties: firstly, citizens whose identities were exploited by scammers, leading to adverse impacts on credit history, requiring significant effort to rectify, and managing ensuing consequences. Secondly, MFIs suffer losses from unrecovered loans to fraudsters, alongside reputational risks. The frequency of such attacks has risen notably since 2022. During 2022-2023, the pinnacle of attempted fraudulent borrowing from a major microfinance company ranged from 350,000 to 700,000 instances, equating to approximately RUB 2-4 billion in loan volume. Despite thwarting over 98% of such transactions, MFIs will soon need to enhance identification and anti-fraud protocols for online loan provision. The Bank of Russia actively engages with the professional community on these matters.

To enhance consumer safety and mitigate the risk of fraud in the online borrowing process, a law[4] has been proposed to heighten the financial liability of banks for fraudulent transactions. Notably, as of July 2024, a two-day "calm down" period has been instituted, during which banks will refrain from transferring funds to suspicious accounts listed in the regulator's database.

This grace period enables individuals to reconsider loans, identify potential fraud, and decline transfers. Should a bank transfer funds before the two-day period lapses, it will be obligated to compensate the client for losses incurred. Additionally, the law mandates banks to deactivate remote service access for individuals implicated in the withdrawal and laundering of stolen funds, following information provided by the Ministry of Internal Affairs of Russia. Citizens will also have the ability to shield themselves from fraudulent borrowing by prohibiting any loan or credit agreements in their name. This legislation will come into effect on March 1, 2025, enabling citizens to issue or revoke self-prohibition through the Public Services portal. In instances where a creditor extends a loan despite the prohibition, it forfeits the right to demand fulfillment of the borrower's obligations.

In view of the growing spread of remote formats with financial services consumers and the strong media coverage of crypto-assets and digital currencies, countering unfair practices may shift almost entirely to the online segment of the financial market.

[3] Information Letter of the Bank of Russia on increased caution by credit organizations towards transactions with parties exhibiting signs of illicit activities on the financial market dated December 27, 2023 No. ИН-08-12/69.

[4] Federal Law on Amendments to Federal Law on Credit History and Federal Law on Consumer Credit (Loan) dated February 26, 2024 No. 31 FZ.

THE USE OF DIGITAL TECHNOLOGIES IN THE COLLECTION, PROCESSING AND SYNTHESIS OF INFORMATION, ANALYTICAL AND OTHER DATA

USED IN PROSECUTORIAL ACTIVITIES: "ELECTRONIC PROSECUTOR'S OFFICE"

OLEG KIPKAYEV,
Head of IT & Information Security Supervision unit, General Department of Supervision over Compliance with Federal Laws of the General Prosecutor's Office

The Electronic Prosecutor's Office IT system (EPO), currently in development, aims to streamline inefficient workflows associated with collecting and processing of large amounts of data in the General Prosecutor's Office (GPO) of the Russian Federation through the use of modern digital technologies

This initiative responds to the pressing need to modernize traditional prosecutorial methods in light of the rapidly evolving digital landscape, necessitating the adoption of more efficient and effective tools for analytical and supervisory tasks. Key drivers for the development of novel software and hardware solutions include:

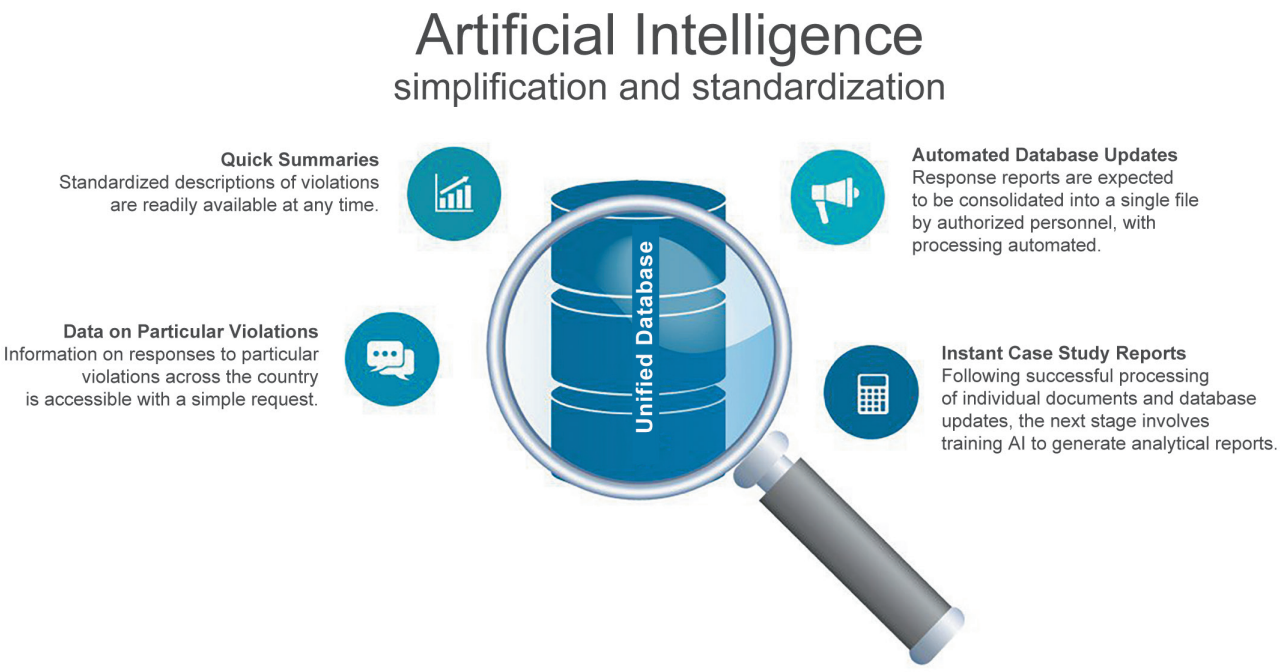
1) **Data Management:** The increasing volume of data adds strain to prosecutors' workloads, necessitating automation tools for effective management.

2) **Analytics:** Time-consuming report preparation hampers prosecution workflows, with the analysis of extensive data becoming progressively challenging.

3) **Big Data:** prosecution authorities handle a fraction of available information. Such information may be employed in the creation of specific documents, but its full potential is thus rarely realized.

4) **Supervision:** Prosecutors need visual information on current deadlines, while dealing with supervision lists is not always practical.

The EPO seeks to automate (including in the future with use of artificial intelligence technologies) the processes of collecting, processing, accumulating, summarizing and analyzing information about the state of law and order, about the practice of supervisory and other activities of prosecutors.



Primary data units will comprise prosecution responses, order execution reports, and other documents that generative AI can process, such as by analyzing the essential features of the corresponding text files. The data array uploaded into the system will be used to generate customizable summary reports, which may then be manually processed if necessary.

For example, in evaluating supervision in public utilities, the EPO platform will identify appeals, protests, lawsuits and other violation reports based on defined criteria. The platform will then produce analytical reports encompassing specific regions and the country as a whole.

However, there are challenges regarding the specifics of computer text processing that necessitate fundamental solutions.

The structure and content of prosecution responses can vary dramatically in different prosecutor's offices, depending on local specifics, the predominant pattern of information presentation, the abundance of law extracts in documents, including those not directly related to the identified violations.

This is an impediment to the intelligent processing of such responses using machine learning methods designed to work with structured data and a unified logic of information presentation, and therefore, necessitates a change of the specifications for such documents.

In the future, EPO adoption will allow all prosecution authorities to generate prosecution responses with a unified structure, enabling computer processing for analytical reports and forecasts.

Individual system modules that handle structured data without requiring complicated processing have already been placed into trial operation and are being tested.

The current version offers the ability to sum up numerical values (one click, with logic checks). This function was used to generate tables for individual jobs, confirming the facilitation and great speeding of routine work. In the future, thanks to the use of advanced data processing tools, the management of the General Prosecutor's Office will get status updates on the state and dynamics of supervision and other activities more quickly, especially in the absence of reporting data. This, among other things, will improve the quality of managerial decisions.

Another functioning component is the Electronic Job Calendar, which allows to track the timeliness of order execution and the instant search for order sources. It will later transition into the official electronic register for all current jobs. Non-registered documents will be considered unenforceable, reducing organizational burden and reallocating resources to core prosecutorial functions.

This calendar can be implemented across all prosecution authority levels.

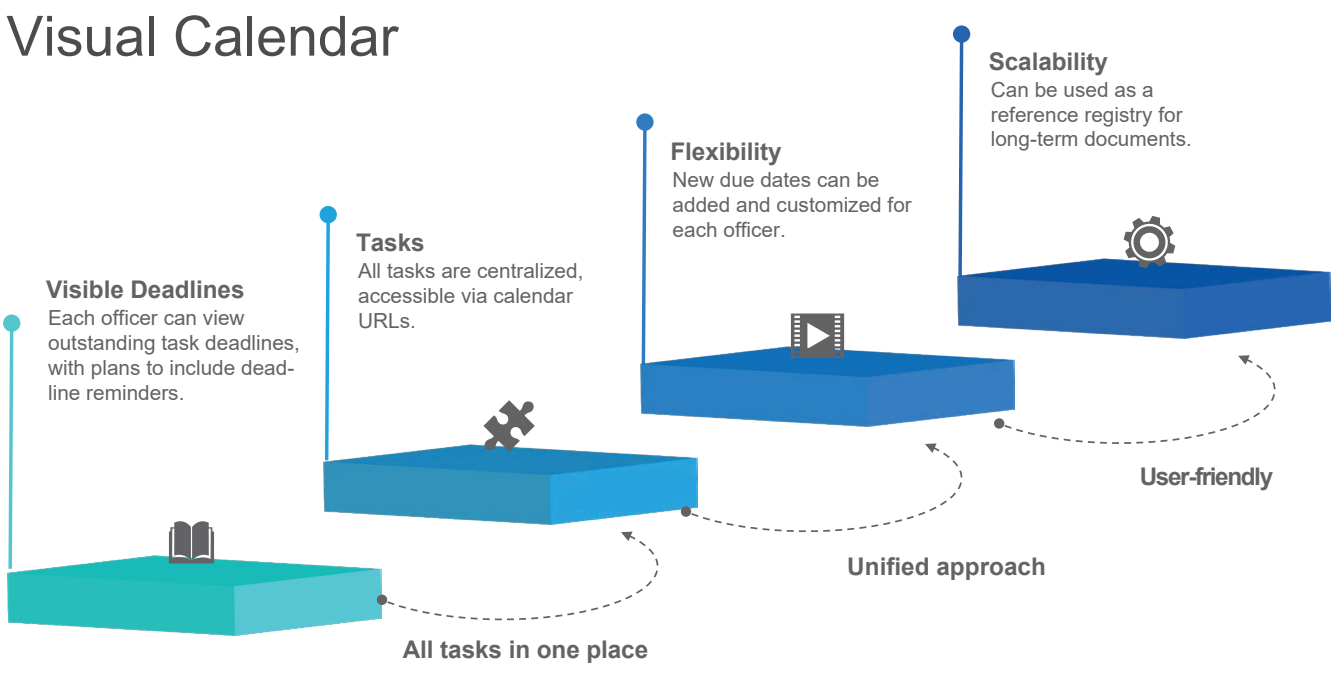
The Kurgan region became the first to test the functionality of the EPO platform. Employees of the Kurgan Prosecutor's Office have been able to insert hyperlinks to documents registered on the Nadzor-WEB platform. This enables employees not only to view information about due dates but also to access the document establishing the due date directly.

Currently, developers are working on electronic report templates for various areas of work. These templates will follow a logical and thematic structure, with character limits to ensure conciseness. Additionally, they will offer additional settings for standard templates to expedite the search and processing of information.

This approach will provide:

1) Secure data storage and analytical capabilities. The acquired data can eventually be utilized to train artificial intelligence, as information is stored in the database.

2) Instant report search and more efficient use of acquired data and their accumulation through end-to-end search.



3) Record keeping of correspondence on a certain subject, ensuring continuity of supervision reports in case of staff changes.

4) Aggregation of reporting data by categories using the established structure to facilitate information processing based on the volume of an analytical job, enabling simpler aggregation of reports using specified parameters.

The EPO platform includes specialized modules that have already proven useful in prosecutorial activities, such as those linked with the Russian Internet Blacklist (RIB).

According to the letter of the First Deputy General Prosecutor of the Russian Federation dated April 12, 2023 on improving the effectiveness of report and claim preparation in blocking illegal content on the Internet, prosecutors should use the RIB to verify web addresses and avoid duplicating response measures.

Prior to the use of the RIB to generate reports for submission to the GPO on websites advertising forged documents granting rights or releasing from responsibilities, the prosecutorial response efficacy was less than 15%. This was attributed to the duplication of websites requested for inclusion in the blacklist.

For example, around ten prosecutors could report the same website, for example diplom.com, resulting in redundant efforts across regional offices to review the website and compile the required package of documents.

With the RIB operational, the efficiency of individual prosecutors in the trial zone increased to 50-70%. Once all prosecutors join the RIB system, this indicator is expected to spike to 95%.

Another registry, the registry of public contracts signed within the Digital Economy National Project framework, now plays a vital role in enhancing the quality of supervision.
Prosecutors can access this register via the EPO portal and acquire information on the corresponding public contracts in their region without having to submit specific requests. Rosfinmonitoring sources the data and updates it quarterly.

Lower-level prosecutors became acquainted with the register's capabilities from the information letter of the First Deputy General Prosecutor of the Russian Federation dated July 31, 2023 on the intensification of prosecutor's supervision over compliance in the implementation of the Digital Economy National Project.

As a result, the EPO platform has already become a valuable electronic assistant for prosecutors at all levels. Further updates will unleash the full capabilities of this product, which has the potential to dramatically change traditional ways of organizing prosecutorial activities by relieving employees from handling purely technical tasks and allowing them to focus on intellectual data processing. Ultimately, this will enhance supervision quality and safeguard citizens' rights and freedoms.

CRYPTOCURRENCY: FINDING SOLUTIONS

LEGAL REGULATION OF THE CIRCULATION OF VIRTUAL ASSETS AND COMBATING THEIR USE FOR ML/TF PURPOSES IN INDIVIDUAL EAG COUNTRIES

Over the past 15 years, the landscape of virtual asset relations has undergone significant transformations due to the development of distributed registry technology. This evolution has given rise to mixers, tumblers, and anonymizers, facilitating the concealment of transactional ownership. Additionally, there has been a proliferation of virtual asset service providers[1], including those operating in the shadow sector, alongside a manifold increase in the number of cryptocurrencies

OLGA TISEN,
Head of Legal, Federal Financial Monitoring Service, Doctor of Law, Co-chairman of EAG Working Group on Evaluations and Legal Issues

The first international document to address the subject of new digital settlement entities was the Financial Action Task Force (FATF) Report on Virtual Currencies, released in June 2014[2]. It outlines key definitions related to the operation of virtual assets and the associated risks identified at the time. It also documents the subsequently reconfirmed thesis that virtual currencies in the hands of criminals are a powerful new tool for transferring and holding funds in ways that are beyond control of law enforcement and other competent authorities.

A year later, in June 2015, FATF issued Guidelines for a Risk-Based Approach to Virtual Assets, outlining strategies to mitigate the risks of money laundering and terrorist financing associated with digital currencies.

In October 2018, FATF standards were extended to cover financial activities involving virtual assets, with updates issued annually since 2021. In 2020, FATF issued a report on signs of money laundering and terrorist financing associated with the turnover of virtual assets, as well as a Report for G20 finance ministries and central banks on the issue of stablecoin[3].

These efforts culminated in the establishment of an international regulatory framework, urging states to adopt regimes for the turnover of virtual assets to combat security threats posed by the use of cryptocurrencies[4] by transnational

[1] Virtual Asset Service Provider is any individual or legal entity that conducts, as a business activity, one or more of the following transactions for and/or on behalf of another individual or legal entity: exchange between virtual assets and fiat currencies; exchange between one or more forms of virtual assets; transfer of virtual assets; holding and/or administering virtual assets or instruments enabling control over virtual assets; engagement in and provision of financial services involving the offer of the issuer and/or sale of a virtual asset // Virtual Currencies. Key definitions and potential risks in AML/CFT: FATF Report, June 2014

[2] Virtual Currencies. Key definitions and potential risks in AML/CFT: FATF Report, June 2014 // www.fatf-gafi.org

[3] www.fatf-gafi.org.

organized criminals, particularly for money laundering and terrorism financing purposes[5].

CLEARLY, INTRODUCING REGULATORY FRAMEWORK FOR VIRTUAL ASSET SERVICE PROVIDERS, APPLYING THE INTERNATIONAL AML/CFT STANDARDS TO THEM OR COMPLETELY BANNING VIRTUAL ASSETS IS AN UNAVOIDABLE REALITY FOR ALL STATES.

The fundamental requirements of the FATF standards regarding virtual asset turnover include:

- Identification, assessment, and mitigation of money laundering and terrorist financing risks associated with virtual asset transactions;
- For the purposes of applying the FATF standards, virtual assets should be classified as property, which entails their classification as the subject of crimes, including ML/FT offenses. Virtual assets as property are subject to blocking (freezing), seizure, and confiscation;
- The activities of virtual asset service providers that carry out exchange, transfer, and safekeeping of virtual assets must be monitored, including registration/licensing and supervision of such entities. Virtual asset service providers should be obliged to identify clients, their beneficial owners, to report suspicious transactions to FIU, as well as to store data.

The FATF's October 2021 Guidelines on Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers stipulate that states may ban or restrict virtual asset operations or virtual asset service providers based on risk assessment and national laws, as well as other policies, such as consumer protection, security and stability, and monetary policy[6]. If a state opts to ban or restrict activities with virtual assets in the country, the FATF Recommendation 15 will not apply in that regard, but jurisdictions will have to assess the resulting risks. In case of violation of the ban, the states that adopted such a decision will have to take relevant measures against the violator (paragraphs 108, 109 of the Guidelines), as well as identify individuals and legal entities operating virtual assets without registration and license.

UN Security Council Resolution 1617 mandates compliance with FATF standards and comprehensive international standards as reflected in the FATF Forty Recommendation on Money Laundering and Nine Special Recommendations on Terrorist Financing.

When it comes to implementing the FATF Recommendation 15, there are three primary models for regulating virtual asset turnover:

1) Banning virtual asset turnover and their use as a means of payment in the country;
2) Legalizing virtual asset turnover, including their use as a means of payment, and developing relevant markets and infrastructure;
3) Regulating virtual asset turnover, while imposing legislative restrictions on their use and regulating virtual asset service providers. This model is the most common in the world.

While most countries have established regulations governing the legal status of virtual assets within their jurisdictions, such as permitting or banning their use for payments, ownership, and investment, the process of legally classifying virtual asset service providers as AML/CFT entities has been slower in many nations. This classification is crucial as it enables authorities to prevent the misuse of cryptocurrencies by criminals and enhances efforts to combat illicit activities in the digital asset space.

All three models are applied by EAG countries. Mainland China banned the use of cryptocurrencies in 2017; Belarus, India, Kazakhstan, Kyrgyzstan, and Uzbekistan have already classified virtual asset service providers as AML/CFT entities. The Russian Federation regulates digital asset service providers. Tajikistan and Turkmenistan are currently in the process of developing regulations in this regard.

REPUBLIC OF BELARUS

Belarus established the legal status of virtual assets in 2017 by the Decree of the President of the Republic of Belarus on the Development of Digital Economy No. 8 dated December 21, 2017[7] (hereinafter, "the Decree"). The Decree envisages conditions for the integration of blockchain and other technologies into the national economy based on the principles of

[4] Cryptocurrency in this article means a decentralized convertible virtual currency. The terms "cryptocurrency," "virtual assets," and "crypto-assets" are used as identical in this article.

[5] Annex to the Decision of the Parliamentary Assembly of the Collective Security Treaty Organization dated December 5, 2022 No. 15-6.5.

[6] www.fatf-gafi.org.

[7] https://president.gov.by/ru/documents/dekret-8-ot-21-dekabrja-2017-g-17716

distribution, decentralization, and security of transactions.

According to Annex 1 to the Decree, cryptocurrency means bitcoin, other digital token used in international circulation as a universal means of exchange.

According to the Belarusian law, citizens are allowed to buy and sell cryptocurrency on any crypto exchanges, including international ones. However, legal entities can only engage in such activities with residents of the Hi-Tech Park[8]. Entrepreneurs are allowed to buy and sell cryptocurrency as residents of the Park (paragraph 2.2 of the Decree).

The following business activities of individuals and legal entities, which are not residents of the Park, are prohibited: assisting other persons in performing/executing transactions with tokens in Belarus and/or via the Internet (including as a party to such transactions using an online information system or by authorizing other persons to use it), as well as in acquiring, alienating, exchanging tokens (paragraph 2.6 of the Decree).

The activities of virtual asset service providers in the country are regulated by the Park Administration, the National Bank of the Republic of Belarus, and the State Control Committee. Inspections of Hi-Tech Park residents are not allowed without prior approval of the Administration (paragraph 4.6 of the Decree).

According to the legislation, the following types of business activities are permitted to residents of the Park in Belarus, which according to the FATF standards are classified as virtual asset service providers: crypto exchange, ICO, and mining pool.

All virtual asset service providers operating in the Park are classified as AML/CFT entities and are required implement procedures to comply with anti-money laundering requirements.

REPUBLIC OF KAZAKHSTAN

The ***Republic of Kazakhstan*** regulates the virtual asset turnover by the Law on Amending and Supplementing Certain Legislative Acts of the Republic of Kazakhstan on Regulation of Digital Technologies dated June 25, 2020 No. 347-VI ZRK. Pursuant to this law, digital assets are classified as property, but their use as a means of payment is prohibited in Kazakhstan.

The law on cryptocurrencies divides digital assets into two categories: secured and unsecured. Cryptocurrencies are considered as unsecured assets and their issue and circulation are banned in Kazakhstan, except for the Astana International Financial Center that was established in 2018.

On November 18, 2021, Kazakhstan adopted Law on Amending and Supplementing Certain Legislative Acts of the Republic of Kazakhstan on Anti-Money Laundering and Countering the Financing of Terrorism No. 73-VII ZRK. According to the law, entities engaged in activities such as issuing digital assets, organizing their trading, and providing services for the exchange of digital assets for money, valuables, or other property are classified as subjects of financial monitoring. These entities are required to notify the authorized informatization authority when commencing or terminating their activities, and such information must be recorded in the relevant state register.

The Law of the Republic of Kazakhstan on Amending and Supplementing the Code of the Republic of Kazakhstan on Taxes and Other Obligatory Payments to the Budget (Tax Code) and the Law of the Republic of Kazakhstan on Enactment of the Code of the Republic of Kazakhstan on Taxes and Other Obligatory Payments to the Budget (Tax Code) dated June 24, 2021 No. 53-VII ZRK regulates the taxation of the cryptocurrency mining.

To foster the growth of the digital asset industry, the President of Kazakhstan enacted the Law on Digital Assets in the Republic of Kazakhstan (hereinafter, "the Law") on February 6, 2023; it introduces government oversight, licensing and administration, and taxation measures for digital assets.

[8] Hereinafter, the Park.

The Ministry of Digital Development, Innovation, and Aerospace Industry of the Republic of Kazakhstan is designated as the authority responsible for determining the legal framework governing the turnover of digital assets. According to the Law, the issuance and circulation of unsecured digital assets, as well as activities involving digital asset exchanges with unsecured digital assets, are prohibited in Kazakhstan, except within the Astana International Financial Center. The Center serves as a "regulatory sandbox," overseeing digital asset service providers and the turnover of digital assets.

In addition to overseeing the turnover of digital assets, the Astana International Financial Center regulates various digital asset service providers, including crypto exchanges, brokers, dealers, custodians, fund managers, and advisors. To prevent digital asset service providers from being exploited for money laundering and terrorist financing, they are required to implement Know Your Customer and Know Your Transaction procedures. This entails conducting due diligence not only on their clients but also on their clients' e-wallets and transaction histories to identify any violations of anti-money laundering and counter-terrorism financing laws.

Entities engaged in issuing digital assets, organizing their trading, or providing services for the exchange of digital assets for money, valuables, or other property are classified as subjects of financial monitoring under Article 3 of the Law on Anti-Money Laundering and Countering the Financing of Terrorism. The Chairman of the Financial Monitoring Agency of Kazakhstan has issued a decree approving rules for the submission of data and information on transactions subject to financial monitoring by such entities, including signs of suspicious transactions involving digital assets.

Kazakhstan places a particular emphasis on regulating mining pools, which are classified as virtual asset service providers by the FATF[9].

KYRGYZ REPUBLIC

The ***Kyrgyz Republic*** enacted the Law on Virtual Assets dated January 21, 2022 No. 12, which came into force on July 28, 2022, to regulate the circulation of cryptocurrencies. This law provides definitions related to the regulated area, establishes the legal status of virtual assets, and outlines requirements for parties involved in cryptocurrency transactions.

Entities involved in the circulation of cryptocurrency, as defined by the law, include virtual asset service providers, virtual asset trading operators, cryptocurrency exchanges, mining pools[10].

According to paragraph 19, part 1, Article 5 of the Law of the Kyrgyz Republic on Anti-Money Laundering and Countering the Financing of Terrorism dated August 6, 2018 No. 87[11] (hereinafter, "the Law No. 87"), virtual asset service providers are classified as financial institutions that are obliged to conduct due diligence on clients, report suspicious transactions to the State Financial Intelligence Service under the Ministry of Finance of the Kyrgyz Republic, and adhere to internal control measures for combating money laundering and terrorism financing.

Pursuant to Articles 16, 18, 25, 28 of the Law of the Kyrgyz Republic on Virtual Assets, the Cabinet of Ministers of the Kyrgyz Republic adopted the Resolution on Regulating Relations Resulting from Turnover of Virtual Assets dated September 16, 2022 No. 514. According to Article 2 of the Law on Amending Certain Legislative Acts Regarding Virtual Assets dated August 5, 2022 No. 81, amendments were made to the Law No. 87. Virtual asset service providers have been classified as financial institutions and subject to all requirements of the Law No. 87 and the FATF Recommendation 10-21.

All virtual asset service providers must obtain licenses in the Kyrgyz Republic, which are issued by the Financial Market Regulation and Supervision Service under the Ministry of Economy and Commerce of the Kyrgyz Republic. Only legal entities registered in Kyrgyzstan are eligible to apply for these licenses.

The relationship between the State Financial Intelligence Service of the Kyrgyz Republic and operators of e-payment systems are also regulated by the Law No. 87 and the Regulation on the procedure for submission of information and documents to the Financial Intelligence Authority of the Kyrgyz Republic (approved by the Resolution of the Government of the Kyrgyz Republic dated December 25, 2018 No. 606). Virtual asset service providers are mandated to comply with these Regulations when implementing Know Your Customer (KYC) checks.

After 15 years of the existence of cryptocurrencies, we clearly see that legal gaps in regulation of their circulation create new threats to economic security and increase the risks of their misuse by criminals.

Read the continued article on how cryptocurrency circulation is regulated in other CIS and BRICS countries in the next issue.

[9] Item 5, Article 11 of the Law of the Republic of Kazakhstan on Digital Financial Assets // https://online.zakon.kz/m/document/?doc_id=33689356
[10] http://cbd.minjust.gov.kg/act/view/ru
[11] http://cbd.minjust.gov.kg/act/view/ru-ru/111822?ysclid=loiruxojbb75473943

AML INVESTIGATIONS IN THE WEB3 INDUSTRY

Over the past decade, the financial landscape has undergone significant transformation due to the emergence of cryptocurrency, paving the way for the formation of an alternative financial system. While not all transactions within this system are illicit (accounting for less than 0.5%), the prevalence of crimes remains notably high

DMITRY MACHIKHIN,
International expert on payments and AML (AML/CFT) in Web3, Member of the Expert Council on Cryptocurrency Legalization of the Russian State Duma

The majority of offenses involve money laundering, terrorist financing, other types of fraud, hacking, and theft. To address these challenges, various technological tools have been developed to monitor, investigate, and combat these threats.

In this article, we will look at the strengths and weaknesses of existing AML solutions in the cryptocurrency market, as well as several ways for identifying cryptocurrency address owners and assessing the frequency with which virtual assets are used for illicit purposes.

AML HISTORY IN CRYPTOCURRENCY

During the early emergence of cryptocurrencies like Bitcoin, there were no AML regulations in place, leading to the proliferation of anonymous darknet markets such as Silk Road.

At this stage, regulatory norms were limited to general laws governing administrative, criminal, and tax matters, with little oversight of online transactions. However, some legal trading platforms began implementing Know Your Customer (KYC) procedures voluntarily, inspired by traditional financial regulations.

In June 2014, following the investigation and arrest of Silk Road's founders, the Financial Action Task Force (FATF) recognized the seriousness of the issue and the rising popularity of cryptocurrencies.

The FATF then issued its report1 Virtual Currencies: Key Definitions and Potential AML/CFT Risks, which detailed the potential danger of money laundering via cryptocurrencies.

It was not until five years later, in 2019, that the FATF issued[2] its first guidelines, which impacted both virtual asset service providers and the cryptocurrency market as a whole.

The regulator's guidelines establish foundational principles for AML regulation in the cryptocurrency market and delineated the roles and responsibilities of public authorities in enforcing these regulations.

[1] Virtual Currencies: Key Definitions and Potential AML/CFT Risks [Online] // FATF. Available at https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf.coredownload.pdf (accessed on February 20, 2024)

[2] Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers [Online] // FATF. Available at https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets.html (accessed on February 20, 2024)

CRYPTO CRIMES: TYPES & STATISTICS. ROLE OF CRYPTOCURRENCY

Despite its appealing potential for democratizing financial systems, cryptocurrencies have also been exploited by criminal elements for various illicit activities. Various tokens, including Bitcoin, are frequently involved in a wide range of crimes.

Cryptocurrency is utilized to legalize proceeds of crime, fraud, and extortion. Among the tokens commonly involved in criminal activities, stablecoins like Tether (USDT) or USD Coin (USDC) are preferred due to their low volatility and peg to the US dollar.

Criminals often resort to impersonating celebrities to gain the trust of their victims. Thus, unknown individuals stole over $160,000 from their victims on several blockchain networks by deepfaking an American entrepreneur on YouTube.

While certain cryptocurrencies offer increased anonymity, making them appealing for cross-border transactions between criminals, there has been a global increase[3] in regulation and scrutiny of such assets.

Cryptocurrency value received by illicit addresses by category. Source: Chainalysis.

According to the American analysts, cryptocurrencies have increasingly appeared in fraudulent schemes since 2017.

Cryptocurrency has been utilized for terrorism financing. Despite large-scale steps to reduce such activity, there are some occasions where the efforts were insufficient.

UNCOVERING ILLICIT CRYPTOCURRENCY: WHAT TO DO IF ONLY THE ADDRESS IS KNOWN

Various ways of identifying and analyzing blockchain transactions are used to detect illicit cryptocurrency operations. The outcome of the investigations, however, depends not only on the AML provider's approach, but also on the methods used by cyber criminals.

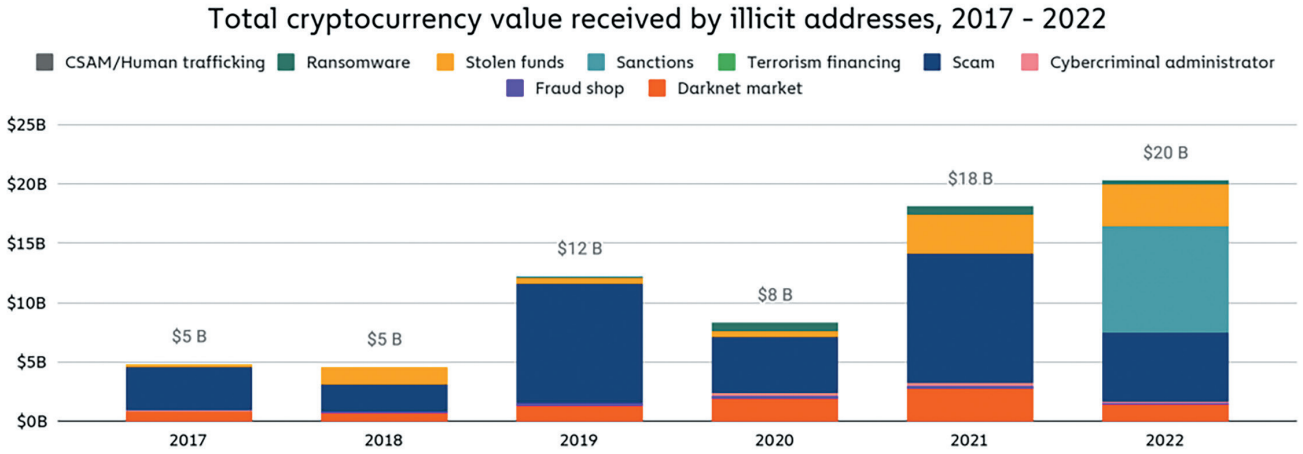
AML providers use a variety of approaches to detect illicit funds. One of the best known methods is the dusting attack[4] that sends small amounts of cryptocurrency on targeted addresses in order to identify the owner of a specific address.

Employees of Chainalysis and CipherTrace have already publicly opposed[5] the usage of such approaches in their work. They do, however, acknowledge that individual blockchain analysts employ such analysis methodologies.

However, blockchain data analysis is not the only approach. Major AML providers typically have a large team of blockchain analytics and forensics professionals who use deterministic methods to identify cryptocurrency addresses.

For example, in the case of cryptocurrency services, analysts may identify deposit and withdrawal addresses to trace the movement of virtual assets across the blockchain network and sometimes even uncover the owner's identity.

▶ **Distribution of cryptocurrency volumes received to "dirty" addresses by category**
Source: Chainalysis

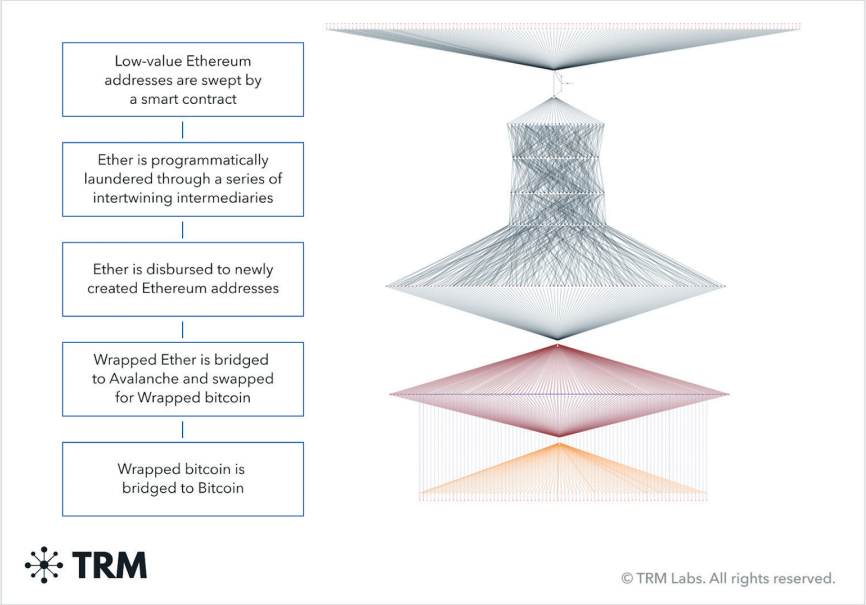


[3] Binance Will Delist ANT, MULTI, Vai, XMR on 2024-02-20 [Online] // Binance. Available at https://www.binance.com/en/support/announcement/binance-will-delist-ant-multi-vai-xmr-on-2024-02-20-f73b083ba6834771b07dbe5319917ae5 (accessed on February 20, 2024)

[4] What is Dusting Attack [Online] // Habr. Available at https://habr.com/ru/articles/450430/ (accessed on February 20, 2024)

[5] Dust Attacks Make a Mess in Bitcoin Wallets, but There Could Be a Fix [Online] // CoinDesk. Available at https://www.coindesk.com/tech/2020/08/18/dust-attacks-make-a-mess-in-bitcoin-wallets-but-there-could-be-a-fix/ (accessed on February 20, 2024)

A scheme to launder stolen ETH and convert them into other tokens to exchange them for BTC
Source: TRM Labs



Identifying a cryptocurrency address in the Bitcoin ATM network. Source: Chainalysis.

AML providers also employ OSINT analytics, which usually means scouring[6] open-source platforms, such as YouTube, Telegram, X (previously Twitter), and Reddit, web forums, darknet, and other similar platforms.

If AML providers know only wallet addresses, they can analyze prior transaction data to identify potential contacts of suspects with centralized services that require customer identification.

Some AML providers also collaborate with law enforcement agencies and cryptocurrency exchanges to enhance their capabilities and speed in identifying offenders.

A growing challenge for AML efforts is the increasing popularity of crypto mixers and decentralized bridges, which complicate the traceability of funds. Tornado Cash, for instance, initially designed for legitimate purposes, became popular among illegal players in the crypto market.

Identifying a cryptocurrency address to a network of bitcoin miners
Source: Chainalysis

AML PROVIDERS: STRENGTHS AND WEAKNESSES, GROWTH AREAS

Despite constant algorithm improvements, AML providers continue to encounter a variety of obstacles. For example, they frequently fail to receive responses from cryptocurrency exchanges.

A large disparity in compliance standards across jurisdictions hampers the work of AML providers on an international scale.

For example, a well-known centralized cryptocurrency exchange publicly admitted[7] that its user was involved in large-scale fraud. The platform, however, did not block the user, citing the absence of a request from law enforcement agencies.

Furthermore, each major AML provider uses unique, secret methods of data analysis and address labeling. On the one hand, it boosts market competitiveness while also aiding in crime prevention. On the other hand, a lack of established standards causes a major disparity in job quality, as well as the possibility to manipulate data and labeling.

In 2021, the FATF turned[8] to a group of AML providers in order to get information on the extent to which virtual assets are used with and without cryptocurrency exchanges. The disparity in the final statistics was so vast that the FATF had to declare that it was impossible to draw meaningful conclusions based on the outcomes.

[6] The Data Accuracy Flywheel: How Chainalysis Consistently Identifies and Verifies Blockchain Entities [Online] // Chainalysis. Available at https://www.chainalysis.com/blog/chainalysis-data-accuracy/ (accessed on February 20, 2024)

[7] KuCoin confirms an exchange user is behind alleged daily rug pulls [Online] // Cointelegraph. Available at https://cointelegraph.com/news/kucoin-meme-coin-daily-rug-pull-confirmation (accessed on February 20, 2024)

[8] Second 12-Month Review Revised FATF Standards on Virtual Assets and VASPs [Online] // FATF. Available at https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Second-12-Month-Review-Revised-FATF-Standards-Virtual-Assets-VASPS.pdf (accessed on February 20, 2024)

With the creation of a unified database of standards and certification of service quality, AML providers would be able to considerably enhance the efficiency of their work while also ensuring the overall security of the cryptocurrency environment.

Insufficient regulation and the lack of harmonized international AML standards pose significant challenges in combating financial crime in the cryptocurrency sphere. The disparate approaches taken by various authorities complicate the work of AML providers and hinder international cooperation in this area.

Efficient financial crime prevention in the cryptocurrency sphere requires harmonized international AML standards for cryptocurrency market regulation. Efforts to standardize regulations, such as those pursued by the FATF, have yet to yield comprehensive results.

Government agencies should be more active in their collaboration with AML providers to streamline training processes and enhance the quality of work.

It is also vital to train AML professionals so that they can effectively combat financial crimes in the crypto sphere. Advanced training programs and certification courses will assist specialists in acquiring the relevant skills and competencies.

On a side note, discrepancies in data among AML providers, often influenced by political or sanctions reasons, highlight the complexities of the regulatory landscape. For example, an AML provider in the United States may deem a specific wallet sanctioned, yet another provider and the Russian Federation may have opposing data. If such assets appear on a lawful centralized exchange, discrepancies may occur, and funds may be blocked.

CONCLUSION

The reduction in illicit cryptocurrency activity from $39.6 billion in 2022 to $24.2 billion in 2023 is a positive development.

Although the figure remains significant, it pales in comparison to the number of crimes in traditional financial markets[9]. However, addressing crimes in the Web3 industry clearly necessitates an integrated approach. At the same time, it is important to note that this statistic only includes labeled illicit addresses, leaving out transactions in the gray zone, transactions that may violate bank AML standards, and assets hidden from taxation and identification. The exact figure is a mystery, which could significantly inflate the actual amount of illicit activity.

Developing adequate AML procedures alone is insufficient to address the issue. International cooperation and enhanced AML competence among all stakeholders in the cryptocurrency sector participants are equally important.

Nonetheless, AML providers play a crucial role in combating cryptocurrency crimes. They also ensure that the cryptocurrency industry has not become bogged down in regulatory restrictions.

Achieving a balance between security and privacy is essential for effective regulation. AML procedures should not violate user rights while also adhering to privacy and data security norms.

The path to a secure future for cryptocurrencies is difficult but attainable. Improving technologies, expanding international cooperation, and facilitating collaboration among governments, regulators, AML providers, and cryptocurrency companies may all help provide a safe and transparent foundation for the cryptocurrency industry's growth.

[9] 2023 Fraud and Financial Crime Report [Online] // Kroll. Available at https://www.kroll.com/en/insights/publications/fraud-and-financial-crime-report (accessed on February 20, 2024)

NAVIGATING VIRTUAL ASSETS: CRYPTO, NFTS, AND FINANCIAL SECURITY

The digital revolution, marked by the emergence of blockchain technology and cryptocurrencies, has heralded a new era in the financial industry, bringing both opportunities and challenges

SHAWN MUNIR,
CEO and co-founder of the Coinweb.com company (UAE)

As we navigate this landscape, it's crucial to understand the dual nature of virtual assets - while they promise innovation and empowerment, they also present ways for bad actors to misuse them, notably in financing terrorism.

Here is my promise:

You will gain insights into virtual assets or discover practical examples that could transform your work or organization. One insight may be sufficient for a thorough understanding. That's my promise.

I am Shawn Munir, the CEO and Co-Founder of Coinweb.com. Our platform analyzes and compares company and user behavior data across the crypto space.

CURRENT STATE OF CRYPTO

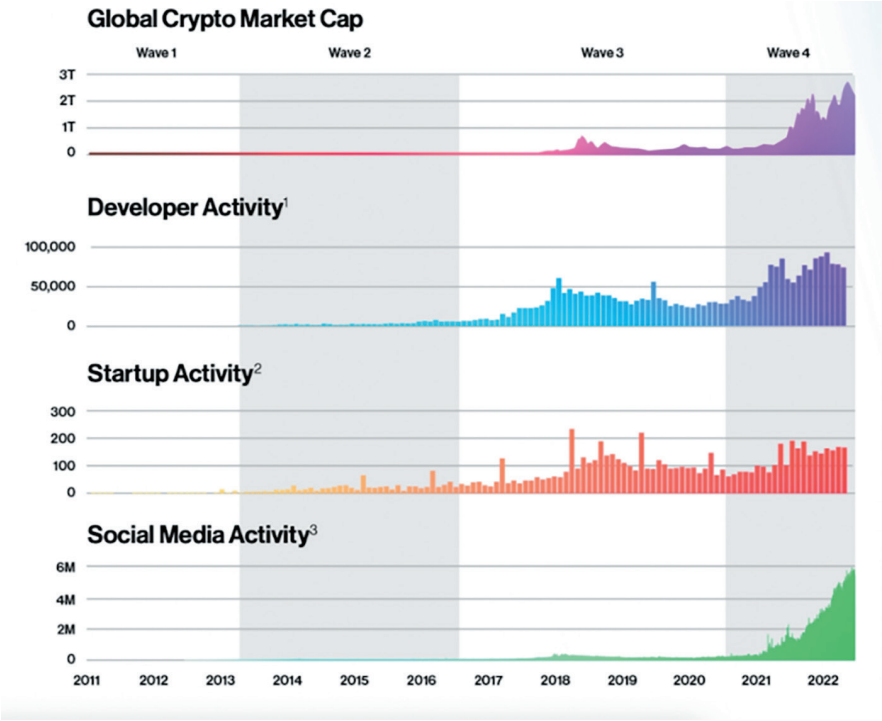
We're in the fourth cycle of cryptocurrency. Despite its seemingly chaotic from the outside, it has an inherent order linked to market capitalization, developer engagement, startup ventures and social media.

Bitcoin ETF was approved in 2024 and Ethereum ETF will follow, coupled with the Bitcoin halving in May 2024 that subsequently starts a bull run.

DeFi, or Decentralized Finance has surged from virtually non-existent to a valuation exceeding $100 billion within two years (2020-2022).

Stablecoins, designed to ensure stability as the U.S. dollar or gold, have gotten significant traction in regions with inflation and currency volatility (especially in Africa, the Middle East, and Southeast Asia).

The NFT market, meanwhile, has exploded, with transactions soaring to $44.2 billion in 2021 from $106 million the previous year. However, this domain is not without its challenges, including wash trading and money laundering.



ANTI-MONEY LAUNDERING AND COMBATING OF FINANCING TERRORISM

Cryptocurrency, often viewed with skepticism, has paradoxically also become the first industry to present a viable solution to money laundering.

This progress is largely thanks to the swift regulatory actions led by the Financial Action Task Force (FATF), a global entity crucial in the fight against money laundering and terrorism financing.

Urgent measures are needed to combat money laundering and terrorist financing. Criminals and terrorists do not wait for regulatory frameworks to catch up.

Private Sector's Call for Regulation

Interestingly, the crypto sector has had a huge demand for regulation. It stems from a network effect in financial markets where entities prefer engaging with regulated counterparts to mitigate risk.

This inclination towards regulation has spurred the development of competitive regulatory solutions, enabling smaller crypto entities to collaborate with traditional financial market players for liquidity.

Despite these strides, the crypto market's capitalization remains modest at $2 trillion, compared to the daily transaction volume of the US dollar at $2.6 trillion.

Private Sector and Regulatory Collaboration

Combatting financial crimes requires a concerted effort to "follow the money." Financial institutions play a pivotal role in this ecosystem, tasked with understanding client activities, spotting inconsistencies, and monitoring transactions.

Suspicious activities must be reported to Financial Intelligence Units (FIUs), highlighting the collaborative effort between the private sector and regulatory authorities in identifying and mitigating financial crimes.

With that as a background – we'll go into the NFTs.

NFTS – THE NEW WAY OF TOKENIZING ASSETS

Non-Fungible Tokens (NFTs) are revolutionizing how we view digital ownership, converting digital data into unique assets on the blockchain.

The movement began with CryptoPunks in 2017, a collection of 10,000 unique pixel art images that inspired the ERC-721 standard, foundational for the NFT and modern crypto art movements.

NFTs and Crimes

With new technologies come new risks. NFTs are no exception, posing potential misuse avenues for criminal activities.

The surge in NFT popularity, especially during the COVID-19 pandemic, has highlighted the necessity for secure platforms and regulatory scrutiny.

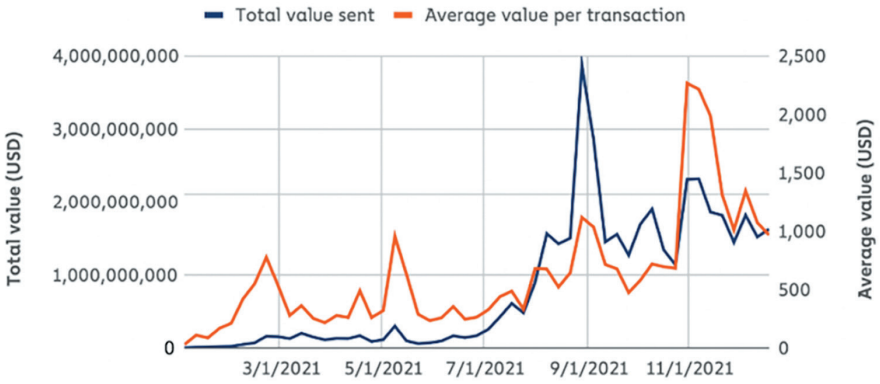
The pandemic and a decline in traditional fine art sales may have redirected investments towards NFTs, with transactions soaring from $106 million in 2020 to over $17 billion in 2021.

TERRORISM FINANCING AND VIRTUAL ASSETS

Terrorist organizations have exploited cryptocurrencies for funding.

Notably, in 2020, Al-Qaeda[1] raised funds through social media, leading to a joint law enforcement seizure of over $1 million.

[1] Terrorist organization prohibited in the Russian Federation.



Efforts to track and flag these transactions have been largely successful, preventing the funds from being laundered through exchanges.

NFTs Spreading Terror Messages

For instance, on September 6, 2022, an NFT was used to disseminate a terror message by IS[2], praising an attack in Afghanistan.

The message originated from IS-KP (Islamic State Khorasan Province), the IS faction active in Afghanistan.

Khorasan Province

By the grace of Allah Almighty, the soldiers of Caliphate detonated an explosive device on a vehicle of the apostate Taliban militia, in the Khugyani area in Nanjarhar, which led to its damage and the wounding of 4 members in it, and praise be to Allah.

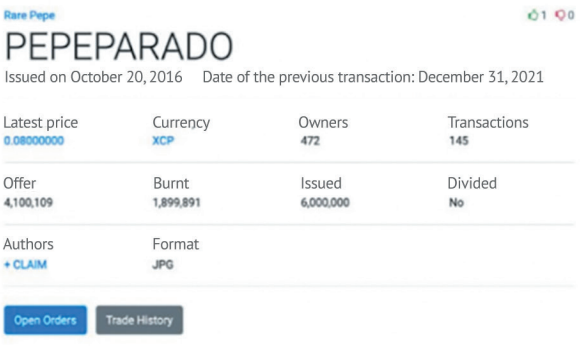
This marked the first use of an NFT for such purposes, with additional NFTs created by the same supporters, exploring the limits of bypassing authority and content moderation on NFT platforms.

NFTs and Far-Right Financing

The "Rare Pepe" NFTs, initially popular memes, were used by the far-right, with a notable case in December 2020 where over $500,000 in Bitcoin was donated to far-right figures.

When checking his wallet, a transaction was discovered where a donation was made to an anonymous Bitcoin-based Rare Pepe crypto collectible holder.

This included a transaction involving a "Rare Pepe" NFT, highlighting the potential for NFTs in financing extremist activities.



IMPLICATIONS

The significance of these events lies in the potential implications for terrorist financing. They signal that groups like far-right terrorists or the Islamic State may be exploring the use of emerging financial technologies like NFTs for fundraising and messaging operations.

The use of NFTs by terrorist groups for value creation and fund reception is not a new concept. The transfer of "Pepe the Frog" NFT and the creation of IS-NEWS #01 seemed inevitable.

Although these NFTs have not been traded, their presence on the blockchain is distributed across countless internet-connected systems. They are virtually immune to action by the Department of Justice or other law enforcement agencies.

Thus, they are as resistant to censorship as possible, which is a serious problem in the fight against extremist online content.

[2] Terrorist organization prohibited in the Russian Federation.

THE URGENCY OF AML/CFT REGULATION FOR VIRTUAL ASSET SERVICE PROVIDERS' ACTIVITIES WORLDWIDE

In October 2018, the FATF expanded its guidelines to include financial transactions involving virtual assets. Since 2021, the FATF Recommendations have undergone annual updates. In 2020, the FATF issued two reports: Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing and the FATF Report to G20 on So-Called Stablecoins

SOFIA RUDKOVICH,
First-year student at Lomonosov Moscow State University; Two-time winner of the International Olympiad on Financial Security (2021 and 2022)

However, despite these developments, many governments throughout the world have yet to implement regulations governing VASP activities. This regulatory gap exposes virtual assets and VASPs to potential misuse[1] and creates barriers to the preliminary investigation of crimes involving virtual assets, such as terrorist financing and the laundering of illicit proceeds. Furthermore, seizing, banning, and confiscating illicit virtual assets, including those intended for terrorism financing, become increasingly challenging.

The FATF Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers contains a full overview of VASPs. A VASP is defined as any natural or legal person conducting one or more of the following activities or operations on behalf of another natural or legal person:

1) Exchange between virtual assets and fiat currencies;
2) Exchange between one or more forms of virtual assets;
3) Transfer of virtual assets;
4) Safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets;
5) Participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset[2].

The FATF Recommendations are mandatory under paragraph 7 of UN Security Council Resolution No. 1617 of July 29, 2005[3]. However, in 2022, the FATF noted that only a limited number of member states had followed the new VASP Recommendations[4].

[1] FATF (2022), Targeted Update on Implementation of the FATF Standards on Virtual Assets/VASPs, FATF, Paris, France: https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Targeted-Update-Implementation-FATF%20Standards-Virtual%20Assets-VASPs.pdf.coredownload.pdf, p. 3.

[2] FATF (2021), Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, FATF, Paris: https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Updated-Guidance-VA-VASP.pdf, p. 109.

[3] UN Security Council Resolution No.1617 of July 29, 2005 (Adopted in New York on July 29, 2005 at the 5244th meeting of the UN Security Council) // SPS ConsultantPlus.

THE FOLLOWING FATF REQUIREMENTS SHOULD BE ENFORCED CONCERNING VAS AND VASPS:

- Adoption of a risk-based approach to VA activities or operations and VASPs;
- Supervision or monitoring of VASPs for AML/CFT purposes;
- Licensing or registration;
- Implementation of preventive measures, such as customer due diligence, recordkeeping, and reporting of suspicious transaction, among others;
- Implementation of sanctions and other enforcement measures;
- Promotion of international co-operation.

The absence of VASP regulation does not hamper their operation. On the contrary, it increases the shadow sector of the economy. A large number of cryptocurrency exchanges operate outside the legal system, remaining unregistered in any jurisdiction, failing to identify the owners of cryptocurrency addresses, and disregarding compliance and regulations. This situation creates opportunities for utilizing cryptocurrencies in criminal activities such as money laundering and terrorism financing without fear of prosecution[5].

The absence of VASP regulation has had particularly severe effects in the sphere of criminal proceedings. There are two primary methods for seizing illicit proceeds in the form of cryptocurrency:

1) By seizing "cold" (hardware) crypto wallets or obtaining the private key of the crypto wallet owner, which grants law enforcement authorities access to illicit proceeds, following investigative actions or criminal intelligence operations;

2) By interacting with the VASP.

In cases where investigative actions or criminal intelligence operations fail to secure the seizure of a crypto wallet or private key, law enforcement authorities can only arrest or block cryptocurrency by making a data provision request to the VASP utilized by the suspect/defendant. They may request the following data: Name, ID, nationality, address, user photo, contact details, IP address, VPN use history, real IP address if anonymization applications were used, geolocation, device identifiers, user statistics, preferences, activity, the recipient's account number, date and time of account creation, exchange operation status, input/output amounts[6]. However, this method is only feasible in cases when the VASP operates legally and verifies its users in accordance with KYC (Know Your Client) guidelines. For example, during client registration, the VASP may require an ID copy and/or an image of the user holding the ID[7].

Virtual asset service providers are often mandated to provide this information in compliance with national regulations. However, this requirement does not always extend to VASPs in foreign jurisdictions, as they may avoid sharing consumer information. Nonetheless, certain countries where legal regulation of VASP operations is extending compel VASPs registered in other jurisdictions to provide data[8].

Due to the substantial hazards associated with the lack of VASP regulation, I believe the following measures are necessary:

1) VASPs should be globally classified as AML/CFT entities and require registration and authorization;

2) Implementation of customer due diligence by VASPs for any one-time transactions exceeding a certain threshold. The FATF Guidance sets this threshold at USD/EUR 1,000.

The 2021 FATF Guidance underscores the significance of international coordination among supervisory bodies, as VASPs engage cross-border activities. Today, as the risks associated with the misuse of virtual assets for illicit purposes grow, governments should unite addressing these new challenges and threats, rather than politicizing anti-crime cooperation.

The final round of the International Olympiad on Financial Security was radically different from the final rounds of other Olympiads on the Approved List, including the All-Russian Olympiad for Schoolchildren, which I won on several occasions between 2020 and 2022.

[4] FATF (2022), Targeted Update on Implementation of the FATF Standards on Virtual Assets/VASPs, FATF, Paris, France, p. 7.

[5] O. Tisen. Identification of crypto wallets' owners, detection and seizure of private keys during criminal investigations.// Criminal proceedings. 2024. No 1, pp. 78-83.

[6] FATF (2021), Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, FATF, Paris, p. 80.

[7] O. Tisen. Methods for identifying and investigating crimes committed using cryptocurrencies. Moscow, 2023. p. 53.

[8] O. Tisen. Tracing cryptocurrency transactions for crime investigation // Criminal proceedings. 2024. No. 2. pp. 54-59, p. 59.

As the winner of the First and Second International Olympiad on Financial Security, I first learned about the Olympiad through social media when I was in the ninth grade, and I was eager to participate. My interest in law developed since the eighth grade, and I was a member of the Moscow Law Team. To prepare for the Olympiad, I researched FATF standards and Russian AML/CFT legislation, as well as watched video tutorials on financial security. Such persistent training enabled me to reach the finals and win.

The final round of the International Olympiad on Financial Security was incredible, inspiring me to aspire to new heights and make decisions about my future career. My favorite part of the Olympiad was the finals, which spanned almost a week, but you only had two hours to complete the actual assignments. The remaining time was devoted to sightseeing, entertainment, and educational activities, which allowed us to become acquainted with the theory and practice of AML/CFT.

The Olympiad's training events are something I will never forget. The criminal process game based on the Soviet film The Diamond Arm, as well as the Income Legalization in Cartoons and Movies Puzzle Quest, not only expanded our knowledge but also provided opportunities to showcase our creativity, acting talent, and communication skills.

I will always remember the meeting with Yury Chikhanchin, Director of Rosfinmonitoring. He is a very exceptional individual and a true professional.

I am fascinated and inspired by our country's history of combating financial crimes. In 2001, our country faced a serious challenge when it was blacklisted by the FATF. Twenty years later, thanks to collaborative efforts, the Russian Federation has developed one of the most effective systems for combatting financial security crimes.

In the future, I hope to pursue a career in financial security as both a researcher and practitioner in this sector.

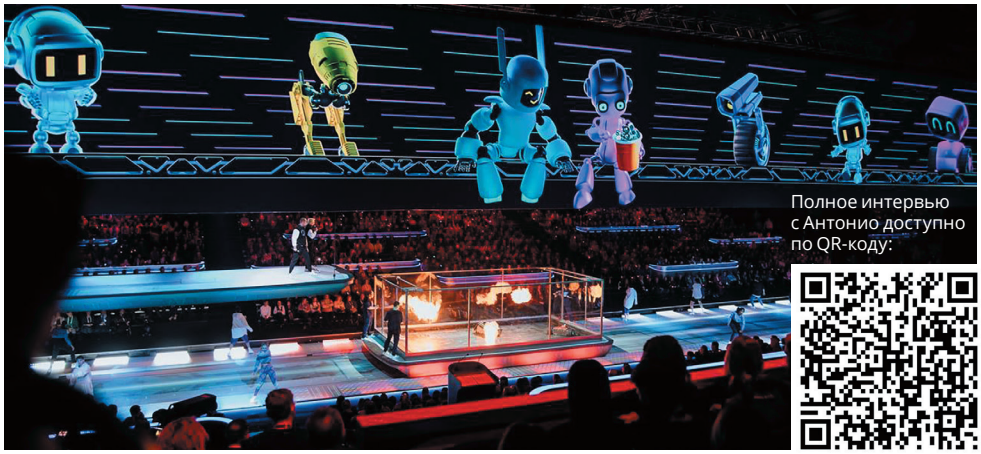
ANTI-MONEY LAUNDERING NEWS

"GAMES OF THE FUTURE". WINNERS OF THE FOUR CONTINENTS CUP TOURNAMENT VISITED KAZAN

The finalists of the III International Olympiad on Financial Security, players from Russia, Algeria, Iran, Cuba, Kyrgyzstan, Tajikistan and Uzbekistan, visited the capital of the Republic of Tatarstan to participate in the "Games of the Future"

Kyrgyzstan, Tajikistan and Uzbekistan, visited the capital of the Republic of Tatarstan to participate in the "Games of the Future".

During the Olympiad finals, the young people achieved the best scores in the phygital soccer tournament, whilst in Kazan they managed to explore other kinds of cybersport. Dmitry Chernyshenko, Deputy Prime Minister of the Government of the Russian Federation, invited the students to attend the "Games of the Future" international multi-sports tournament. One of the guests and participants in the Olympiad, Jordan Antonio Rodriguez, a Cuban, while being a child got to know Russia at a distance thanks to his grandmother who had moved to Cuba in her youth and had never forgotten her homeland. The young man heard many stories about our country and in 2023; he came here to attend the Sirius International Olympiad on Financial Security. We asked Antonio to share his insights into the future of international financial security, "People and governments shall understand that it is crucial in today's highly globalized and technological world to protect one's personal assets and to ensure the security of the country as a whole. I dream of global financial security cooperation, when political, economic disagreements would be set aside, and the countries would be united to eliminate terrorism and to address other issues, such as money laundering, for instance. At present, however, this looks like a utopia." Another two of the participants, Fateh Bousry from Algeria and Bahriddin Rustamov from Tajikistan, continued their journey across Russia and became attendees of the World Youth Festival held in the Sirius Federal Territory. Being involved in the extensive program of the Festival, the young people spared time to share their impressions about the "Games of the Future" and the International Olympiad on Financial Security. "Last year I was a captain of the "Wolves" international team that won the phygital soccer match at the Olympiad on Financial Security. This is the reason we have been invited to Kazan to attend the Games of the Future. And now I am at the World Youth Festival. I would like to not only expand my own knowledge in the field of financial security, but also to share it. Currently, I am fiercely preparing for the next Olympiad; I am willing to go to the finals. Moreover, I am involved in the outreach activities within the Movement Project, trying to spread the word about my country's initiative," said Bahriddin. Some of Fateh's most vivid impressions include meetings with the renowned politicians and athletes from all over the world, "My meeting with Vladimir Putin, President of the Russian Federation, at the opening ceremony as well as the opportunity to watch the event from the VIP box together with the heads of states became the most memorable experience during the Games of the Future. For me it was a great honor and a very good memory. I would like to thank everyone for the hospitality, and would certainly wish to visit Russia again."



Полное интервью с Антонио доступно по QR-коду:

THE FIRST MEETING OF THE BRICS COUNCIL ON COMBATING MONEY LAUNDERING AND TERRORIST FINANCING IN N EXPANDED FORMAT

A video-conference meeting of the BRICS Council on AML/CFT, the first in 2024, was held at the Federal Financial Monitoring Service

During the meeting, discussions focused on enhancing national anti-money laundering systems and continuing collaborative efforts to ensure financial security.

The Russian BRICS Chairmanship presented initiatives aimed at improving the transparency of financial systems, mitigating risks and threats, fostering public-private partnerships, and encouraging young people to contribute to financial security. In particular, projects such as the International Money Laundering and Terrorist Financing Risk Assessment Center, the Transparent Blockchain service, the International Olympiad on Financial Security and the International Compliance Council garnered interest from attendees.

Participants expressed confidence that the BRICS Council on AML/CFT would make a significant contribution to the global anti-money laundering and counter-terrorism financing framework, as well as support the implementation of the BRICS Economic Partnership Strategy 2025.

FINANCIAL SECURITY ISSUES DISCUSSED AT THE WORLD YOUTH FESTIVAL

In March, young people from around the world gathered at a grand event at Sirius

The World Youth Festival welcomed 20 thousand Russian and foreign leaders in business, media, international cooperation, culture, science, education, volunteering and charity, sports, various social areas, along with teenagers representing various children's organizations and associations.

Financial security agenda was an important part of the Festival. Experts from the Federal Financial Monitoring Service, the International Training and Methodology Center for Financial Monitoring and Promsvyazbank presented the Sodruzhestvo platform and hosted a series of events for attendees of the Festival. This included over 50 finalists of the International Olympiad on Financial Security, as well as young financial intelligence officers from other countries participating in the Festival.

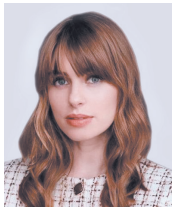
Throughout the Festival, participants learned about the International Olympiad on Financial Security and how to apply for the 2024 Olympiad. They discussed important issues of combating financial crime and shared experiences from their respective countries through debates and business games.

EDITORIAL BOARD

Chairman of Editorial Board
Mr. Yury Chikhanchin

Deputy Chairman of Editorial Board
Mr. Vladimir Ovchinnikov

Deputy Chairman of Editorial Board
Mr. German Neglyad



Chief Editor
Ms. Irina Ryazanova

MEMBERS OF EDITORIAL BOARD

Ms. Galina Bobrysheva

Mr. Ivan Kornev

Mr. Oleg Krylov

Mr. Anton Lisitsyn

Mr. Sergey Teterukov

Mr. Alexey Petrenko

Ms. Margarita Andronova

Mr. Evgeny Gileta

Ms. Marina Shemyakina

Rosfinmonitoring and ITMCFM in Telegram and VKontakte

Publisher
Autonomous Non-Profit Organization
International Training and Methodology Centre for Financial Monitoring
Staromonetny Lane 31, bld.1,
Moscow, Russia, 119017. E-mail: info@mumcfm.ru.

ITMCFM
2024