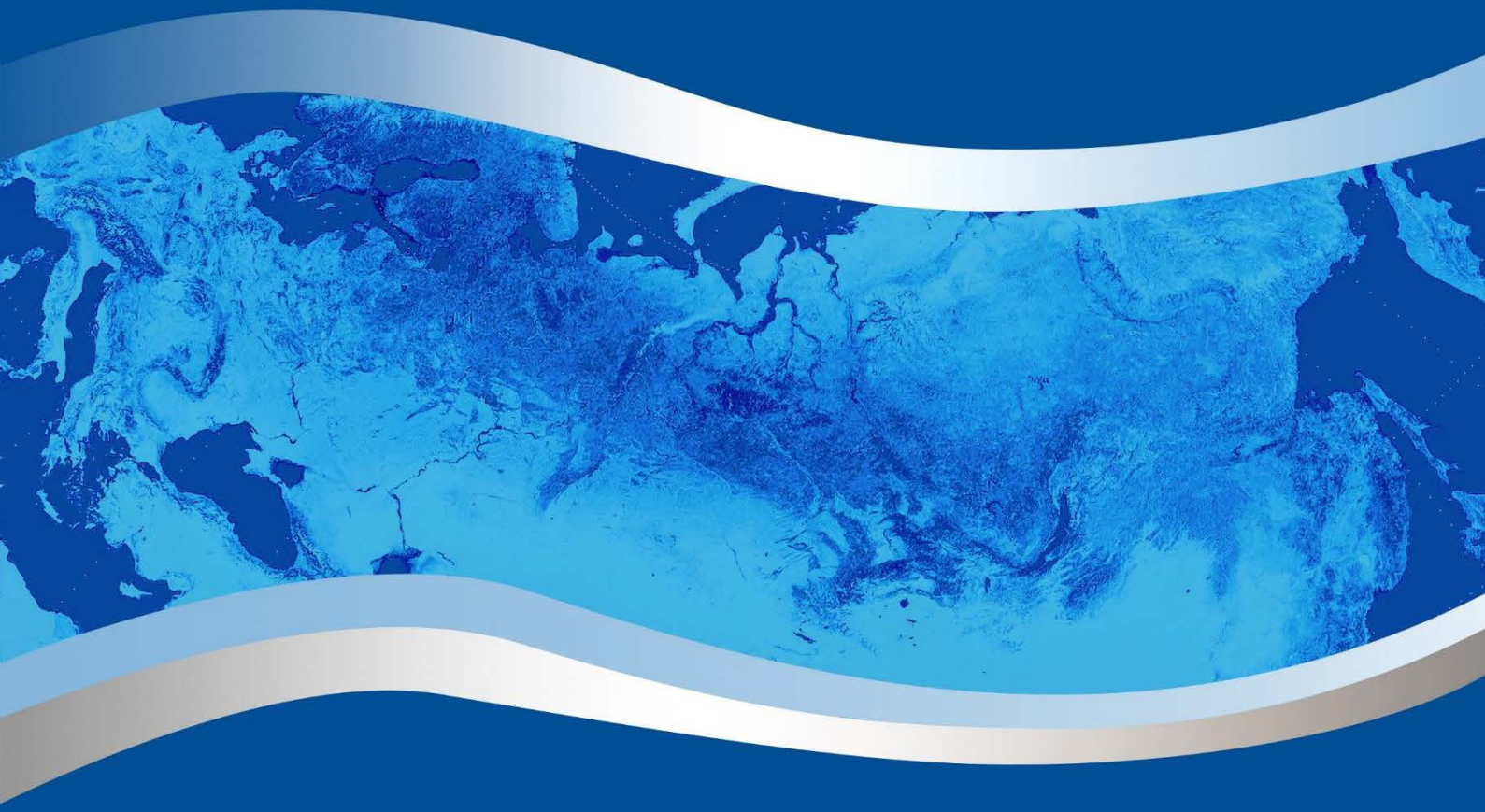
ЕВРАЗИЙСКАЯ ГРУППА
по противодействию легализации преступных доходов и финансированию терроризма

EURASIAN GROUP
on combating money laundering and financing of terrorism



EAG TYPOLOGY PROJECT

TYPOLOGIES OF THE USE OF PREVENTIVE MEASURES OF FINANCIAL INSTITUTIONS FOR CRIME DETECTION AND RISK ASSESSMENT

TYPOLOGICAL STUDY REPORT

2021

Contents

General

Application by entities engaged in transactions with funds or other assets of preventive measures as well as identification of suspicious transactions and submission of suspicious transaction reports (STRs) to the financial investigation units (FIUs) is one of the most important measures aimed at mitigating ML/TF risks.

The mutual evaluations of a number of the member states of the Eurasian Group on Combating Money Laundering and Financing of Terrorism (EAG) under the second round have revealed certain areas of concern that should be addressed, which includes the need for improving the regulatory framework and streamlining the law enforcement practice.

In order to address the findings of the international experts, most countries need to take measures for enhancing the effectiveness of application of enhanced and special measures and targeted financial sanctions as well as for improving the effectiveness (quality) of suspicious transaction reports.

The mutual evaluation practice shows that ineffective suspicious transaction reporting regime affects the rating of Immediate Outcome 6 which assesses the effectiveness of the use by competent authorities of financial intelligence and other meaningful information for conducting ML and TF financial investigations and, therefore, undermines the efforts undertaken by financial intelligence units.

On the other hand, continuous extension of the list of information used for conducting strategic, tactical and operational analysis is critical for ensuring effective operation of the FIUs in modern world.

In this context, the study summarizes the approaches and best practices of countries related to the use of STRs as well as the information on preventive measures applied by financial institutions for identifying offences and assessing risks is of high relevance and importance.

Based on the outcomes of discussion of the interim results of the typology study at the WGTYP meeting in November 2020, it was decided to extend the scope of the study to include information on approaches used by countries for providing feedback and on specificities of supervision and implementation by reporting entities of preventive measures amid the spread of the COVID-19 coronavirus infection.

Preventive Measures and Suspicious Transaction Reporting in the EAG members

With the view to mitigate ML/TF/PF risks, financial institutions of the EAG member states may apply the following measures:

- Refuse to carry out a transaction for a customer;
- Refuse to provide access for a customer to online banking services, suspension/ termination of online banking services;
- Refuse to enter into a banking services agreement with a customer;
- Terminate a bank account (deposit) agreement;

- Freeze (block) funds or other assets;
- Suspend transactions with funds or other assets;
- Other

The main preventive measures, that have proved their effectiveness in mitigating ML/TF risks in practice, is refusal to carry out transactions for customers and refusal to enter into bank accounts (deposit) agreements with customers (hereinafter referred cumulatively as denial of services to a customer or service denial).

Consistent application of such measures makes it possible to decrease the extent of involvement of financial sector entities in dubious transactions. For example, the restrictive measures applied by the Russian banks prevented movement into illegal turnover of nearly RUR 190 billion in 2019 and over RUR 200 billion (approximately EURO 2.2 billion) in 2020.

The grounds for denial of services due to AML/CFT reasons should be clearly specified in the high-level regulations and national AML/CFT legislation and should be understood by entrepreneurs and companies that use the banking services.

Of interest is the practice whereby the competent authorities provide clarifications to the business community as to the potential exercise by financial institution of the right to refuse to carry out a transaction (enter into a bank accounts (deposit) agreement) due to ML/TF reasons, along with sanitized examples (case studies).

Increased level of awareness of the business community about the AML/CFT legislation enables business entities to more effectively respond to situations when banks apply enhanced CCD measures and to justify absence of higher risks related to a particular transaction or deal.

On the other hand, it allows for reducing the level of de-risking where financial institutions indiscriminately and unreasonably terminate or restrict business relationships with individual customers and entire categories of consumers in order to avoid the risks of being engaged in dubious transactions.

Case Study (Russian Federation)

The Bank of Russia has developed, jointly with the professional business associations, the Methodological Guidelines that describe the actions of businesses that could lead to restriction of access to remote baking services, e.g. online banking services, or to refusal to carry out transactions/ enter into bank account agreements, and also the steps to be taken by businesses to clarify the reasons for refusal to carry out transactions/ to enter into bank account agreements. The Methodological Guidelines were highly assessed by both business community and financial institutions[1]

The most common reasons for denial of services include the following:

[1] The Methodological Guidelines are available of the Bank of Russia website at: https://cbr.ru/Content/Document/File/87237/meth_rec_20190626.pdf

- Information is available indicating that the bank, including non-resident bank, with which the recipient's account is opened, or the recipient of funds are linked to illegal financial transactions or are subject to sanctions;
- There are suspicions that the bank account (deposit) agreement is being entered into by a customer for the money laundering or terrorist financing purposes.
- A customer attempts to open anonymous bank accounts or accounts in fictitious names;
- A financial institution is unable to identify a customer after applying effective CDD measures, or a customer refused to be subject to CDD measures;
- The validity of the ID document of a customer has expired and the customer unreasonably refuses to extend the validity of the ID document;
- Irrational behavior of a customer, attempts to open an account that is inconsistent with his/her/its business purposes;
- A financial institution reasonably suspects that a customer is involved in illegal activities, etc.

In most EAG members, financial institutions notify the relevant competent authorities of preventive measures applied by them.

The trends showing the increase in number of service denials by financial institutions for mitigating ML/TF risks observed in some EAG members may indicate both the high demand for these instruments and the growing effectiveness of measures taken by financial institutions for identifying high-risk transactions.

The incoming reports on denial of services due to ML/TF suspicions is used by the competent authorities and financial intelligence units in the course of financial investigations as well as in the process of conducting strategic, tactical and operational analysis.

Figure 1: Dynamics of Number of Service Denials due to AML/CFT Reasons in Belarus

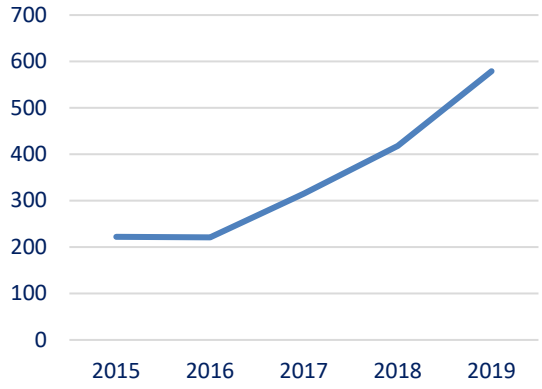


Figure 2: Dynamics of Number of Service Denials due to AML/CFT Reasons in Kyrgyzstan

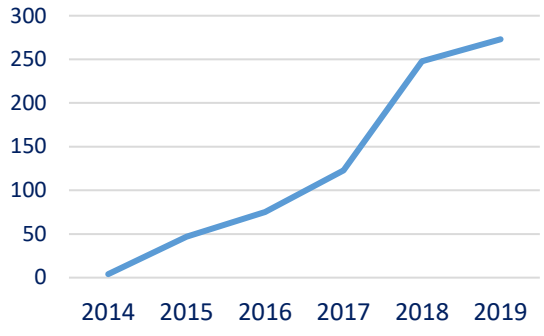
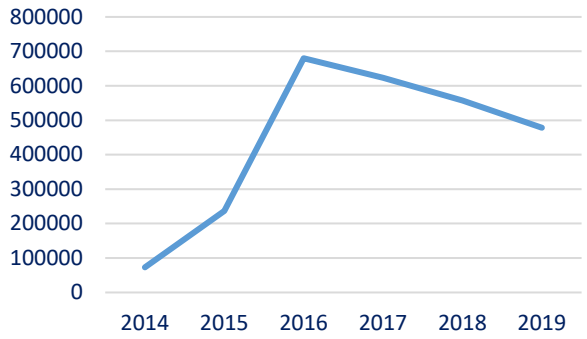


Figure 3: Dynamics of Number of Service Denials due to AML/CFT Reasons in Russia



Some countries indicated that they do not maintain the service denial statistics, stating, inter alia, that this type of statistics is not directly required by FATF Recommendation 33.

In some countries, the measures, such as refusal to carry out transactions for mitigating ML/TF risks, are applied very rarely. The reasons for non-application of this instrument require further analysis.

In general, the mixed trends related to number of STRs submitted by reporting entities are observed in the EAG members. Presented below are the diagrams showing the STR dynamics based on information provided by the EAG members.

Figure 4: Dynamics of number of STRs in Kyrgyzstan

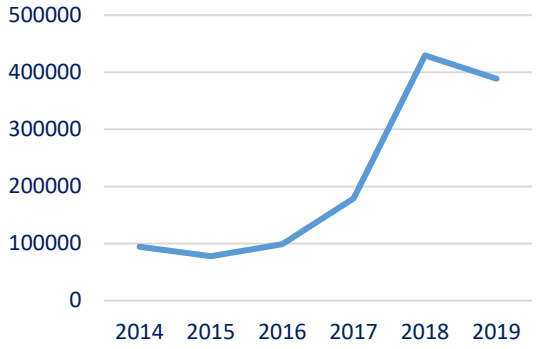
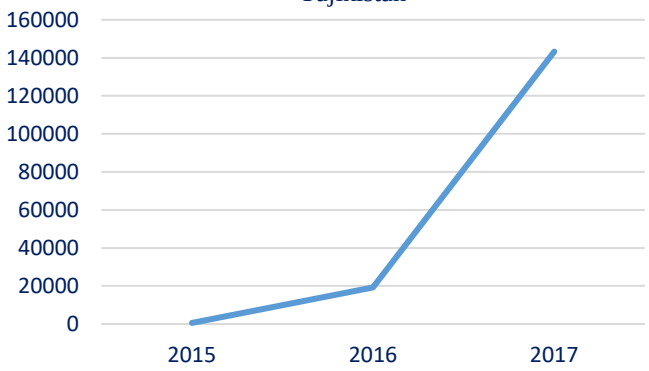


Figure 5: Dynamics of number of STRs in Tajikistan



In some cases, the countries associate the increase in the number of STRs with the growing number of reporting entities that report suspicious transactions, and also with the improved effectiveness of financial monitoring as a result, inter alia, of the feedback provided by the FIUs and the supervisory (competent) authorities. This correlation is particularly obvious in the DNFBP sectors (real estate agents, dealers in precious metal and precious stones, notaries, etc.).

Figure 6: Dynamics of number of STRs in Belarus

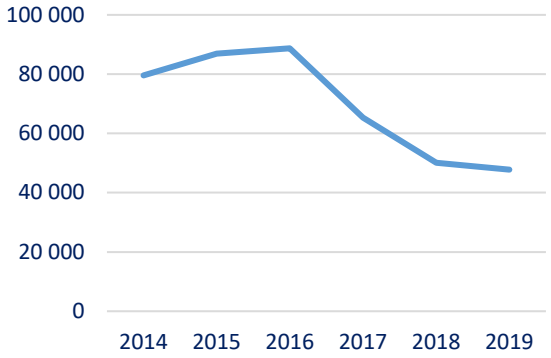
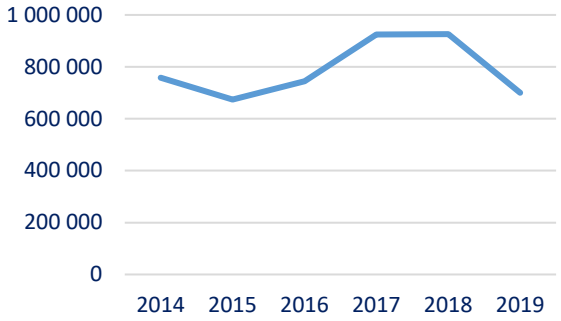


Figure 7: Dynamivs of number of STRs in Kazakhstan



On the other hand, the decline in the number and volume of STRs may indicate the decreased level of involvement of the financial sector entities in dubious transactions and the reduction of size of the shadow economy. It could also indicate the more efficient selection by banks of transactions to be reported to the FIUs, the improved quality of analytical work conducted by the AML/CFT units and the decreasing level of defensing STR filing.

Dynamics of number of STRs in China

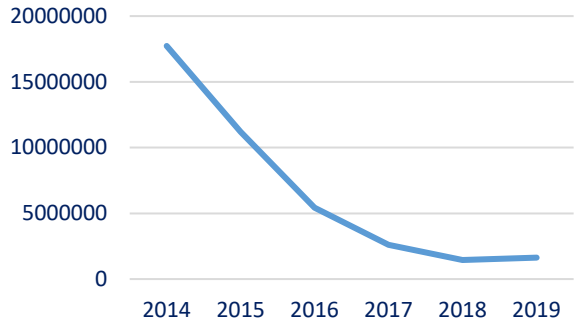


Figure 9: Dynamics of number of STRs in Russia

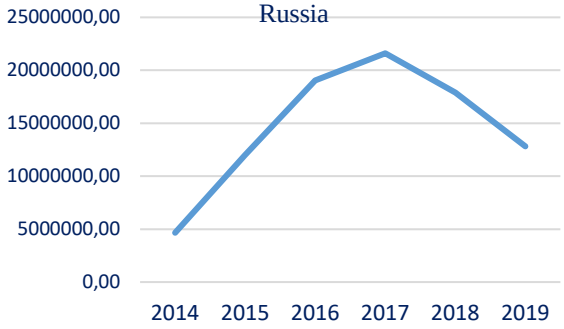
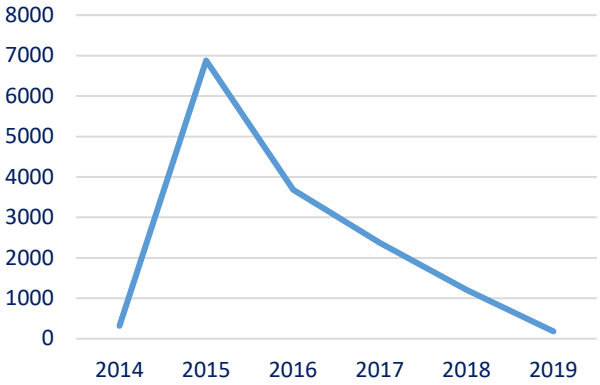


Figure 10: Dynamics of number of STRs in Turkmenistan



The filed STRs should contain at least the following:

- STR registration details;
- Information on financial institution that files STR (identification data);
- Information on each party to a transaction (identification data);

- Information on originating bank and beneficiary bank;
- Transaction details (date, amounts, purpose, type, form, account numbers);
- Reasons for suspicion (description, suspicious transaction code).

In some EAG members, the electronic reporting form includes the special field entitled “Additional Information”, which can be used for more detailed description of the grounds for qualifying a transaction as suspicious one and for indicating other transactions related to the suspicious transaction (description of schemes involving multiple parties), etc.

In some EAG members, the STR form also includes information on beneficial owners of customers and IP and MAC addresses of devices used by customers for accessing online banking services. Such information enables the FIUs to identify additional links and make thematic collections of the incoming STRs;

The customer profile information allows for using the so-called Fingerprint technologies to aggregate multiple data not only based on customer data collected in the process of identification, but also through the use of matching IP-addresses and details of registration and remote access devices (MAC addresses of devices) and patterns of other data footprints left by users of the applied software.

For example, with the view of identifying suspicious transactions and customer activities, financial institutions use the models based on analysis of the aggregate hardware and software solutions used by customers, such as: browser (type, name, version, list of installed plug-ins, list of supported languages), fonts (name of fonts installed on an end-user computer), monitor (display resolution, scratch space resolution, monitor color depth), such as BrowserFingerprint. The practice shows that the aggregate data will be individual and distinctive for almost each device. After the data are passed into the hash function, a fixed-size alphanumeric string is generated, which essentially is the unique digital identifier of a customer.

Having such information, one can distinguish different unusual situations, for example, when a user uses multiple devices, or multiple users use one device, and identify matching devices of users whose transactions have been qualified as suspicious, etc.

Of note is also the practice of using (testing) the special suspicious activity reporting (SAR) form or mini-profiles containing analysis of suspicious activity of customer(s) in some EAG members For example, in Kyrgyzstan, if based on the results of ongoing monitoring and analysis of transactions/ activities of customers a bank becomes suspicious of a certain patterns of transactions, the information with detailed description of the customer transaction pattern, along with all available documents related to the customer activity and account statement, is sent in hard copy to the FIU.

This format has certain advantages and disadvantages compared to the standard STR forms. For example, the suspicious activity reporting (SAR) form enables to include information about interrelated transactions (patterns of transactions) into one report. The practice where financial institutions are permitted to file both STRs and SARs is apparently the optimum option. However, before such option is set out in the legislation, the new reporting mechanisms should be tested in the frame of pilot projects or regulatory sandboxes.

<u>Recommendations:</u> It is suggested to the EAG members to:

1. Analyze the practical exercise by financial institutions of the right to refuse to carry out transactions and the right to refuse to enter into bank account (deposit) agreements as the risk mitigation measures, and take steps for streamlining such practice where necessary (focus financial institution on more active application of preventing measures for mitigation ML/TF risks, develop guidelines and recommendations for financial institutions and other businesses).
2. Consider maintaining various statistical data on number of service denials by reporting entities and volume of denied transactions. Such statistics may be used for analyzing trends in the process of national risks assessments and other reviews.
3. Consider incorporation in the electronic STR from of information on beneficial owners of customers and IP and MAC addresses of devices used by customers for accessing online banking services and also special codes for flagging STRs that require urgent response measures.
4. Countries that have not undergone the mutual evaluation yet should consider introduction of amendments into the AML/CFT legislation to ensure proper implementation of the FATF Standards related to identification and reporting of suspicious transactions to FIU (Recommendations 10 and 20), including:

    - Incorporate provisions that permit financial institutions to file STRs instead of pursuing the CDD process in situations when they suspect ML or TF and reasonably believe that performing the CCD process will tip-off customers;
    - Ensure that not only completed suspicious transactions, but also attempted suspicious transactions are properly reported.

Approaches Used by FIUs for Analyzing Incoming STRs and Service Denial Reports

STRs are one of the main sources of information used for conducting strategic and tactical analysis and generating analytical reports. Differed reference codes and indicators used for categorizing STRs and the STR forms completed by financial institutions enable to collect detailed information on transaction parties and payment purposes, determine volumes and directions of financial flows both domestic and incoming from/ outgoing to foreign (including offshore) jurisdictions, identify sectors, industries and groups causing the highest suspicions, and obtain information of specific risk areas or segments that require enhanced attention.

Service denial reports are essentially the STRs, but more focusing on risks. The difference between these two types of reports from the FIU analysis perspective

is that in case of submitting STRs the customers concerned are now aware of the fact that the STRs has been filed and even do not suspect that they are subject to the enhanced due diligence process2.

Service denial reports, as the preventive measure taken by reporting entities to mitigate ML/TF risks, may be used by supervisors for assessing risks of their supervised entities. For example, the situation, when one reporting entity that is subject to primary financial monitoring (e.g. a bank) refuses to provide services to other reporting entity (e.g. real estate agent), may be indicative of weak internal controls and high risks associated with the activity of the latter.

FIUs may inform supervisory authorities about refusals by credit institutions to provide services to their supervised entities. Supervisory authorities, in turn, may effectively use this information for assessing risks and applying the risk-based approach.

Case Study (Russian Federation)

Rosfinmonitoring disseminates online the information to the supervisory authorities about risks associated with the activities of their respective supervised entities, using for this purpose the supervisors' Personal Account on the Rosfinmonitoring website. This information includes various analytical data demonstrating the general risk dynamics in the sectors (broken down by regions, types of activities and segments), diagrams showing the dynamics of volumes of STRs filed by banks in respect of their customers, and information on preventing measures applied against customers. Besides that, in respect of each entity supervised by other authorities, Rosfinmonitoring provides the integrated risk assessment (high, significant, moderate and low risk) and information under different criteria underlying the risk rating (such as denial of services, filed STRs, failure to timely use (download) the List of persons linked to terrorist activities, etc.

The STRs are primarily used for identifying and preventing ML/TF and predicate offences, initiating financial investigations and responding to information requests received from law enforcement agencies.

In the course of preliminary checks and financial investigations, reports on refusal by financial institutions to carry out financial transactions and/or open accounts for customers serve as the additional criteria pointing, along with other red-flag indicators, to potential suspicious activities of the targeted persons. This information may be included in responses, requests and reference materials and information notes disseminated to the law enforcement and oversight authorities as well as to foreign FIUs.

In the EAG member states, the designated government authorities use very similar approaches and algorithms to analyze and categorize STRs in terms of types of criminal offences and priority for processing the incoming information.

[2] In this case, the provisions of FATF Recommendation 10 are applied according to which, if the institution reasonably believes that performing the CDD process will tip-off the customer or potential customer, it may choose not to pursue that process, and should file an STR.

The FIU analysts use multi-purpose software for analyzing the intelligence and apply data collection tools for analyzing the reports, which includes data requests, export and cross-checking, early warnings, visualization, financial chain tracing and extension and other functions.

In Belarus, the automated high-tech software tools are used and continuously upgraded for processing the information flows. For example, the so-called "electronic cards" (profiles) of entities are maintained in the special software system. This system accumulates all information concerning entities of any types received by the FIU. New information received by the FIU, including information on STRs and service denials, is fed into each card (profile).

Case Study (Republic of Belarus)

The Main Directorate for Combating Organized Crime and Corruption of the RB Interior Ministry received information proactively disseminated by the Belarusian FIU on suspicious financial transactions involving changes in the authorized capital of the Belarusian commercial banks. The criminal intelligence and detective operations conducted in 2014-2015 succeeded in disruption of criminal activities of the executive officers of the commercial bank. who, through misuse of their position and carrying out financial transactions through the accounts of the controlled companies and securities transactions, misappropriated the funds of the foreign bank in the exceptionally large amount, converted the stolen funds into foreign currency (amounting to Euro 5.5 million) and further laundered the criminal proceeds by contributing the above funds to the authorized capital of a newly established bank.

The IT products and elements of artificial intelligence are extensively adopted and used in the analytical work for automated processing of information flows. For example, in the People's Republic of China, the FIU uses different models for verifying and categorizing all incoming STRs in terms of priority and types of criminal offences, including illicit drug trafficking offences.

Case Study (People's Republic of China)

It was established that Mr. Zhang established four companies in Shanghai, Jiansu Province, and in Marshall Islands and instructed his employees to produce narcotic drugs with the use of neuroactive substances and unregulated pharmaceutical raw materials. The companies published information of their supplies, accepted online orders and produced medical drugs in the laboratories of the companies located in the UK, Australia and America, and even seconded their personnel to the UK to assist in production of medicines. The Chinese FIU analyzed the suspicious activities of Mr. Zhang and shared the intelligence with the Russian FIU. Based on the received intelligence, the Russian competent authorities detected the crime and seized the illegal proceeds.

In Kyrgyzstan, the FIU also conducts preliminary analysis and screening of the incoming STRs. After that, the received information is analyzed in-depth,

financial investigations are conducted, and summarized findings are disseminated to the law enforcement agencies.

Case Study (Kyrgyz Republic)

The performed monitoring revealed the incoming STRs concerning the individual entrepreneur, after which the preliminary analysis of those transactions was conducted. The analysis identified the transactions involving regular deposits of funds to the same account and the structured transactions involving transfer of funds by the customer to one or several counterparties with indication of the same payment purpose within the short period of time. After that, the information requests were circulated to the commercial banks that provided services to the individual entrepreneur. According to the received responses, the individual entrepreneur held several current and deposit accounts. The identified transactions were carried out by the individual entrepreneur since 2012 through 2018. The taxes paid by the individual entrepreneur were inconsistent with the turnover of her business. In this situation, additional summarized information was disseminated to the State Service for Combating Economic Crime indicating the needs to recalculate the amount of additional taxes and deductions payable by the individual entrepreneur (income tax, sales tax and value added tax).

In the course of pre-trial proceedings, the tax audit was conducted in respected of the individual entrepreneur, as a result of which the overdue tax amount was fully recovered.

In the Russian Federation, in order to facilitate the analysis of incoming reports on transactions carried out across different sectors of the economy, the electronic "Industries Reference Book" detailing the types of activities of business entities (based on a single categorization system) was developed and built in the Rosfinmonitoring's information system, which allows for performing analytical work taking into account sectoral and regional characteristics and specificities of entities.

External information received through the interagency cooperation channels and the special registers, such as the "Register of Public Procurement Contracts" and "Register of Treasury Transactions", are used for analyzing transactions of entities involved in the public procurement process.

In the process of strategic analysis of transaction flows, enhanced attention is paid to number and volume of transaction reports with due consideration for direction of transactions (incoming, outgoing, regional and inter-regional flows) in the following context:

- Dubious (suspicious) nature of transaction flows;
- Transactions carried out through high-risk banks;
- Involvement of shell companies in transaction flows;
- Involvement of persons who are subject to financial investigations in transaction flows;
- Transaction flows incoming from/ outgoing to countries included in the FATF "grey" and "black" lists, etc.

The flexible system settings allow for adjusting the approach to collection of datasets depending on the priority objectives.

Case Study (Russian Federation)

In 2015, based on the outcomes of analysis of over 300 financial transaction reports forwarded to the Rosfinmonitoring information system, the analytical materials were disseminated to the law enforcement agencies concerning Mr. E who was the director of the company involved in performing the contracted work funded from the federal budget. Rosfinmonitoring suspected Mr. E in misappropriation and legalization of over RUR 5 billion. Based on the Rosfinmonitoring's findings, the investigation agencies initiated the criminal proceedings for money laundering.

In the Republic of Tajikistan, the STRs filed by reporting entities with the FIU are, first of all, categorized in terms of their priority, i.e. the incoming reports are subdivided into four risk categories – very high, high, medium and low risk. After that, the STRs falling into the very high and high risk categories are disseminated by the information processing unit to the executive officer who, in turn, circulates these reports to analysts for conducting operational analysis.

Case Study (Republic of Tajikistan)

After processing the STRs concerning a group of persons filed by the credit institution based on the following criteria: "customer regularly carries out transactions just below the threshold value" and "customer carries out tractions that have no economic rationale", the FIU conducted the analysis of these persons and their transactions. The analysis revealed that this group of persons regularly received a large number of money transfers in small values from the foreign country. Additional investigation established that this group of persons was not registered as individual entrepreneurs or directors, shareholders and founders of companies, and almost all members of this family were unemployed, but owned the real estate property, cars, etc. After the relevant information was disseminated to the Drug Control Agency under the President of the Republic of Tajikistan, the law enforcement agencies established that the funds received by this group from the foreign country were the drug trafficking proceeds. Based on these findings, the criminal proceedings were initiated against a number of persons under several Articles of the Tajik Criminal Code, including Article 262 (Laundering of Criminal Proceeds).

In some EAG members, the analytical work involving strategic analysis is performed by the FIUs, inter alia, in the framework of certain projects. For this purpose, one of the important sectors of the economy exposed to risk is selected, and the FIU conducts analysis of transactions carried out in this sector by institutions, companies and organizations that are part of the same group or the same financial and business structure, e.g. controlled by the federal government authority.

Case Study (Republic of Uzbekistan)

Analysis of the STR related to several transfers of funds by the business entity A to the bank cards of two individuals as the loan for the purchase of residential property revealed that these transactions were aimed at illegal misappropriation of the state budget funds. In particular, the government-owned company B, which business involved collection and storage of non-ferrous metals, bought the real estate property that belonged to the business entity A at the price several times higher than the market value of this property. The director of the government-owned company B was at the same time the beneficiary of the business entity A that sold the real estate property. For concealing the origin of the funds received from the government-owned company B, the business entity A transferred those funds to the bank cards of the close relatives of the director of the government-owned company B as the loan for purchasing residential property, after which the funds were withdrawn in cash.

The use of the special financial criminal profiles related to such risk areas as terrorist financing, illicit drug trafficking, corruption, etc., has proved to be highly effective in the EAG members. Information on suspicious transactions identified based on the aggregate indicators (transactional, behavioral, etc. triggers) is, in general, highly focused on risks and links to predicate offences.

Strategic analysis of incoming STRs is conducted on a regular basis and enables to identify targets for tactical analysis and proactive financial investigations. Besides that, additional incoming STRs allows for recalculating the values of the criteria and indicators in the special calculation panels developed for determining the level of money laundering risk in different financial institutions, sectors and regions.

In the process of strategic research and analysis, some countries have tested the big data analysis techniques with the application of business intelligence technologies (for analyzing data segments) and the artificial intelligence-based technologies, i.e. machine learning, recommender system (or forecasting).

In 2014-2019, the Belarusian financial intelligence unit implemented a number of strategic research projects, including:

- Analysis of STRs related to international money transfers. The actions undertaken by the law enforcement agencies based on the findings of this research resulted in detection of a number of corruption and money laundering-related offences and in recovery of over EURO 5 million to the state budget;
- Misuse of shopping malls for laundering criminal proceeds (based of the research findings, the tax offences were detected and the evaded taxes were recovered to the state budget);
- Identification of schemes of obtaining and (or) laundering of criminal proceeds in the housing and utility sector. The research identified the widespread scheme used by the executive officers of a number of utility companies for receiving bribes;

- Identification of foreign companies established for the money laundering purposes (the research project is ongoing).

Based on the findings of research projects implemented in the framework of strategic analysis, analytical review reports are generated in some EAG members.

In the Republic of Tajikistan, strategic analysis of financial flows linked to laundering of drug trafficking proceeds was conducted, and the analysis findings were disseminated to the Drug Control Agency under the President of Tajikistan.

The countries rank STRs in terms of the main risk areas identified by the NRA. In this case, the STR flow is used for measuring the risk level dynamics, and the relevant STR statistics may be effectively used **in the process of national and sectoral risk assessments**.

On one hand, the indicators, such as number of sector entities that report dubious transactions carried out by customers, and number of reporting entities that deny services to customers, may indicate the level of understanding of ML/TF risks by the sector entities (especially by DNFBPs) and the level of their awareness of the requirements of the AML/CFT legislation.

For this purpose, the countries quite often use the STR concentration index (indicator):

$$I = \frac{Number\ of\ reporting\ entities\ in\ a\ sector\ that\ filed\ STRs\ in\ a\ reporting\ period}{Total\ number\ of\ entities\ in\ a\ sector}$$

The practice shows that active feedback by supervisors and FIUs typically leads to the increase of the index value.

On the other hand, number and volume (value) of suspicious transaction reports and service denial reports filed in respect of entities of a particular sector by banks that provide services to these entities indicate the extent of involvement of the sector in dubious transactions. Therefore, these data may serve as one of (but not the only) indicator for measuring the level and dynamics of risk in a sector.

In Russia, the national ML risk assessment exercise involved the analysis of flows of STRs filed by financial institutions with Rosfinmonitoring. This analysis enabled to determine the shares of suspicious financial transaction reports submitted annually by each financial sector (and, therefore, the main providers of this information were identified). Based on the reported transactions, the main ML and TF threats and risks identified through analysis of other information sources were confirmed.

Of interest is the practice of the People's Republic of China where the supervisors require financial institutions to draw up annual analytical reviews based on the STR statistics. Financial institutions analyze information on customers, their transactions and customer behavior, identify vulnerabilities in their institutions, and subsequently implement targeted risk mitigation measures.

In 2017, the Chinese FIU completed the study of drug-related money laundering typologies based on the received STRs and disseminated the typology

study report to the Chinese National Drug Control Committee. According to the provided information, this typology study has proved to be very useful in combating drug crime and money laundering.

Recommendations: It is suggested to the EAG members to:

1. Consider development of financial criminal profiles related to the prevalent predicate offences (main risk areas) identified in the NRA (e.g. “drug dealer”, “corrupt official”, etc.) containing transactional and behavioral indicators that would enable financial institutions to effectively identify dubious transactions;

2. Consider development (updating) of methodology for assessment by financial institutions of their own risks and vulnerabilities, including analysis of flows of suspicious transaction reports and service denial reports;

3. Consider drawing up reports based on the findings of the aforementioned assessments and disseminating them to the competent authorities for analysis of ML/TF trends and for the use in the process of national and sectoral risk assessments.

Feedback on STRs

The feedback under the Financial Action Task Force standards (Recommendation 34)3 is aimed at assisting financial institutions and designated non-financial businesses and professions in applying national measures to combat money laundering and terrorist financing, particularly in identifying and reporting suspicious operations (transactions).

The main **feedback tool** in the countries is the communication to reporting entities of typologies and indicators of suspicious operations (activities) of customers.

Other feedback tools used by the countries:

- informing reporting entities about the effective use of STRs in financial investigations,
- communicating examples of financial investigations to reporting entities,
- direct meetings with reporting entities.

The following forms of feedback are less common:

- use of online services, Regtech platforms (India, China, Russia),
- posting statistical information on the website about the number of received STRs and their use (Russia).

[3] You can read the FATF Recommendations in the thematic section of the ITMCFM website at https://www.mumcfm.ru/biblioteka/mezdunarodnye-dokumenty/fatf

The Republic of Belarus has developed such form of feedback as training workshops for persons conducting financial transactions, workshops for the personnel of state bodies involved in control activities, advanced training courses, etc.

In the Russian Federation, in cooperation with members of the Compliance Council, Rosfinmonitoring has introduced several formats for providing feedback by reporting entities, namely:

a. Submitting analytical reports on the quality of information interaction containing the following data at least once every six months:

- assessment of timeliness of submitting STRs;
- assessment of informativeness of STRs, as well as their focus on the risks identified during the national risk assessment;
- assessment of compliance of the nature of suspicious transactions, information on which was sent to Rosfinmonitoring, with the classifier of indicators of the unusual nature of transactions;
- assessment of the demand for STRs in certain areas of Rosfinmonitoring activities;
- assessment of the content of responses to requests from Rosfinmonitoring and its territorial bodies sent to reporting entities;
- recommended measures to improve the efficiency of information interaction with Rosfinmonitoring, including recommendations for increasing informativeness and timeliness based on the analysis of specific STRs.

b. Communicating the Information Interaction Quality Index through the Personal Account on the Rosfinmonitoring website.

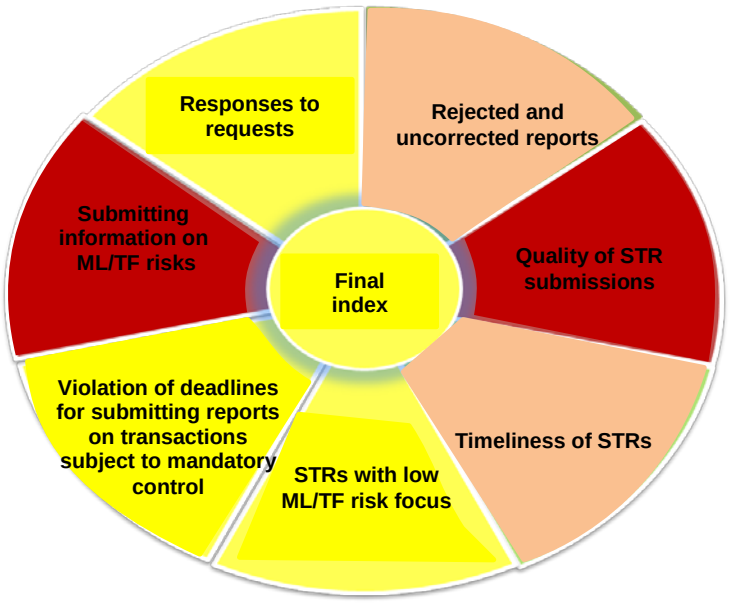


Fig. 11. Information Interaction Quality Index in the reporting entity's Personal Account on the Rosfinmonitoring website

In this case, based on certain algorithms, an assessment is formed of the most significant criteria that characterize the effectiveness of informing (timeliness, focus on risks, characteristics of interaction with Rosfinmonitoring).

Rosfinmonitoring approved the Regulations on the organization of feedback from reporting entities on the basis of the analysis of the information submitted by them.

The quality of information on suspicious transactions is also improved by Rosfinmonitoring efforts to promptly provide information about new risks, typologies and indicators of suspicious transactions. In 2020 alone, more than 20 new typologies were made available to reporting entities through the Personal Account. As interim results of the introduction of new feedback formats, Russia notes an increase in the speed of identifying suspicious transactions, an improvement in the quality (informativeness) of STRs and their focus on risks.

China's FIU conducts an annual assessment of the quality of STRs. The assessment criteria include:

- availability of basic STR elements, including whether customer and transaction data is reported without any errors or omissions.
- a detailed description of operations and the reasons for qualifying them as suspicious, including identities, transactions, etc.
- whether the STR analysis and suspicions are consistent with the evidence specified by financial institution.

Following the assessment, the FIU identifies deficiencies in the reporting system of reporting entities and the process of informing about suspicious transactions, communicates the results to reporting entities, requiring them to improve the STR and CDD regime.

In most countries, feedback is provided by the financial intelligence unit, as the main information user. In some countries, feedback is also provided by law enforcement agencies (Belarus, China, Kyrgyzstan) and supervisory authorities (India, Kazakhstan, Kyrgyzstan, Turkmenistan).

The most important parameters of STR quality in terms of its use by FIUs were defined by the countries as informativeness of STR and timeliness of its submitting.

The supervisory authorities of most EAG members conduct an analysis of the effectiveness of reporting entities in fulfilling their obligations to apply preventive measures and submit STRs.

Among the common violations (issues) identified during inspections of financial institutions are the following:

- incorrect information in messages submitted to the FIU;
- lack of internal documents establishing the procedure for investigating suspicious transactions;

- storage of the check results of customers whose operations are recognized as suspicious only on paper;
- lack of documenting of professional judgments on customer transactions.

To analyze the effectiveness of identifying and reporting suspicious transactions, the FIU usually uses the indicator of timeliness of sending STRs, as well as other criteria, such as the informativeness of STRs, focus on risks, high degree of connection with the predicate crime.

The effective identification of suspicious transactions is usually hindered by:

- insufficient number of algorithms/reports to identify suspicious transactions;
- incorrect algorithms for making reports;
- non-availability of mechanisms/reports to identify customer transactions on the grounds of suspiciousness (frequency of transactions, splitting, depositing large amounts, non-standard purpose of payment, etc).

When assessing the quality of analytical procedures in terms of identifying suspicious transactions and submitting information about them to the FIU, countries use various indicators, including:

- quality of customer identification procedures and customer due diligence, including basic and beneficial ownership information (China), comprehensive examination of customer business relationships before sending an STR, implementation of new IT technologies to identify matches across sanction lists (India, Kazakhstan, Tajikistan).
- clear, complete and logical description of the suspicions on which the STR is based, completeness, accuracy and adequacy of information to identify the suspicion (India, China, Russia, Turkmenistan), high focus on risks and connection with the predicate crime (Kazakhstan).
- timeliness of submitting STRs (India, China, Russia, Turkmenistan).
- decrease in the share of STRs sent automatically according to the established criteria in accordance with the register (range of indicators) of suspicious transactions without conducting an in-depth analysis (Russia, Tajikistan). In this case, countries often use the indicator of the share of false positive responses, i.e., the share of transactions for which red flags were triggered, but which were not qualified as suspicious by responsible persons after the in-depth analysis of transaction and customer information:

$$FP = 1 - \frac{\text{Number of STRs sent to the FIU during the certain period}}{\text{Total number of operations for which red flags were triggered}}$$

For example, in Kyrgyzstan and Tajikistan, on average, only 7% of transactions in the banking sector for which red flags were triggered were submitted

to the FIU after the in-depth analysis. In the Russian Federation, this figure is slightly higher – 10 %.

The practice of the Republic of India to analyze the thresholds set for different AML/CFT scenarios and to review them periodically on the basis of historical data is also interesting.

Competent authorities of a number of countries systematically assess the dynamics of STR quality factors. Almost all EAG members note the positive effect of feedback in terms of improving the quality of STRs, the timeliness of their submitting to the Financial Intelligence Unit.

For example, Rosfinmonitoring tracks the dynamics of STRs with uninformative descriptions. According to the information provided by Russia, there was a 7% decrease in the share of such STRs in 2020 as a result of feedback. There was also a 2% decrease in the share of STRs with poor timeliness of submitting.

As a result of Rosfinmonitoring communicating the typologies to the private sector through the Personal Account, banks have become more effective in identifying the risks highlighted in the National Risk Assessment. According to the information provided by the Russian Federation in 2020, the number of STRs in the "Public sector" and "Illicit Drug Trafficking" risk zones increased.

The Republic of Kyrgyzstan noted a positive effect in orienting banks to high-risk operations in the form of an example of blocking by the bank of an operation worth more than 150 million rubles.

The Republic of Tajikistan as a positive result of feedback from reporting entities notes a significant reduction in the number of errors in submitting STRs, as well as improving the quality of reporting of suspicious transactions.

The Republic of Uzbekistan provided two cases as an example of the effectiveness of feedback in terms of communicating to financial institutions the information about the risks associated with the spread of COVID-19: in the first case the result was the submitting of STRs about the schemes of theft of budget funds allocated by the State to purchase personal protective equipment (disinfectant chemicals) using shell companies. In the second case, the analysis of STRs revealed a scheme of illegal business activities (tax evasion) in the sale of medicines using electronic payment facilities (P2P payments and e-wallets).

The public-private partnership mechanisms in the AML/CFT sphere are playing an increasingly important role in providing feedback to reporting entities from competent authorities, sharing information about new risks and typologies.

In the Republic of Belarus, the FIU conducts training for representatives of financial institutions, including via videoconferencing, involves them in the EAG offsite events, and also takes part in the meetings of the Committee on Combating ML/TF/PF of the Association of Belarusian Banks and in workshops of the Belarusian Chamber of Notaries.

In the People's Republic of China, public-private partnerships are implemented in two forms:

- consultation with intelligence agencies. The FIU invites reporting entities and law enforcement agencies to jointly discuss the financial intelligence data. This format also includes an exchange of views on ML/TF risks and emerging ML/TF typologies or methods.
- joint analysis. The FIU establishes a panel for the financial intelligence data analysis, including both public and private sector representatives, and actively assists in the analysis of financial transactions in complex ML/TF investigations.

The Kyrgyz Republic has a Public Council of the State Financial Intelligence Service, which consists of representatives of civil society.

In the Russian Federation, the main form of interaction with representatives of the private sector is the Compliance Council and the Advisory Council under the Interagency AML/CFT/CPF Commission.

The Compliance Council brings together representatives of services involved in internal control of reporting entities and is a platform for discussing both problematic issues of law enforcement practice and ML/TF risks emerging in the activities of reporting entities.

A body for interaction with the private sector is the Advisory Council under the Interagency AML/CFT/CPF Commission, which includes representatives of major professional associations.

As part of the work of the Advisory Council, the issues of legal regulation of the reporting entities' activities in the AML/CFT/CPF sphere are discussed.

In November 2020, the EAG Plenary meeting approved the establishment of the International Compliance Council (ICC). The ICC, as a mechanism of public-private partnership at the supranational level, will include the heads of AML/CFT departments of the largest banks of the Eurasian region. The main objective of this expert platform is the rapid exchange of information on risks, including those related to cross-border money transfers, as well as the exchange of experience and best practices for identifying high-risk operations and taking measures aimed at the risk mitigation.

Recommendation:

EAG members are invited to consider expanding the formats of feedback provided, including through:

- the use of automated solutions and Regtech platforms for these purposes;
- development of the public-private partnership formats;
- systematization of work on identifying new ML/TF typologies and promptly communicating them to the private sector;
- targeted cooperation with major financial institutions.

Trends and risks in the spread of COVID-19

Most of the EAG member states expressed the view that during the spread of COVID-19 the **volume of the shadow (illegal) economy was shrinking in proportion to the legal economy**.

The following trends have become characteristic of all countries:

- changes in financial behavior due to the rapid growth of online services, the development of e-commerce;
- increase in cybercrime and online fraud;
- States allocating large budgets to fight the pandemic and support the economy and citizens. The onset of the pandemic was associated in several countries with a dramatic increase in the theft of public funds;
- growth of fraud in the production of personal protective equipment, and medicines, as well as in the charity sphere (collection of donations);
- growth of digital transactions (fast electronic payments, P2P transfers, Internet acquiring, etc.);
- growth of activity in cross-border online gambling.

Some countries were also characterized by specific risks, such as fraud in the purchase of airline tickets and online loans (China). The Republic of India noted that the pandemic led to an increase in the availability of financial services. Thus, many businesses began to move out of the shadow economy and make more use of the legal financial system.

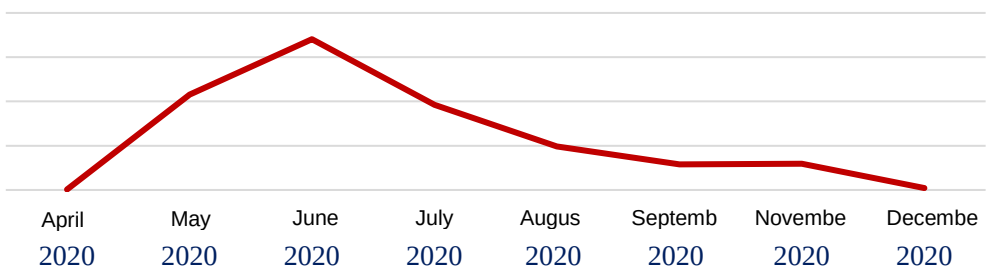
The development of digital platforms (marketplaces) and online commerce has led to an increase in fraud and cyber fraud. With the development of Internet platforms, miscoding (the discrepancy between the declared MCC code and the activity actually being carried out) became active, especially in the segment of illegal gambling business (online casinos).

In a number of countries, unscrupulous practices (fraud) in the financial market have become more active, so-called pseudo-brokers offering citizens supposedly high-yield investment strategies (high returns in a short period of time). Fraudsters take advantage of the difficult economic situation caused by the pandemic, citizens' need for additional income, and their low financial literacy.

EAG members have developed guidelines and recommendations, informing reporting entities about new risks. On the basis of the relevant guidelines, reporting entities have developed indicators and models for monitoring the pandemic-related ML risks which have worked well in practice.

For example, in Russia in April 2020 Rosfinmonitoring together with the Bank of Russia published informational messages on the risks manifested in connection with the coronavirus pandemic, suggesting that reporting entities mark STRs with a special {COVID} marking when these risks are identified. Credit institutions promptly implemented this approach in the work of their compliance departments and actively informed them when relevant risks were identified.

Fig. 12. Dynamics of the COVID-19-related STRs' volume, mln. rubles (Russia)



Most often credit institutions reported the risks of withdrawal of budget funds under the facade of purchasing medical supplies, conducting transit operations under the facade of purchasing masks and protective equipment, cashing out through payroll projects, when "employer" justifies large amounts of money transfers to individuals by providing them material assistance of social nature, manipulation of prices for personal protective equipment. Based on the results of the analysis of the {COVID}-marked STRs submitted by banks, financial investigations and criminal cases on theft and misuse of budgetary funds were initiated.

At present, the results of monitoring of questionable transactions related to the spread of the coronavirus infection indicate a decrease in the corresponding high-risk operations, which may be due to some reduction in the price manipulation risks in the procurement of medicines and personal protective equipment, as well as an increase in the effectiveness of banks' preventive measures.

During the period of the coronavirus infection spread, countries experienced multidirectional trends in STRs. For example, the Chinese CAMLMAC received about 2.59 mln. STRs at the end of 2020, which is 58% more than in the previous year.

The number of STRs in India also increased compared to the previous year. The COVID-19 period saw an increase in the number of STRs. India also attributes the rise in STRs to a surge in so-called digital transactions and an increase in cybercrime.

A number of countries saw a decrease in the number of STRs (Kazakhstan, Tajikistan), which is attributed by the countries to the decline in economic activity and partly to the difficulties encountered by AML/CFT departments in the context of external restrictions and quarantine. In Turkmenistan there were no significant changes in the dynamics of the number of STRs.

Recommendation:

Competent authorities in the EAG members are encouraged to work with the private sector to review current pandemic trends and risks and, if necessary, update relevant guidelines and guidance documents on identifying high-risk operations.

Impact of COVID-19 on AML/CFT supervisory activities and implementation of preventive measures

The coronavirus pandemic and quarantine regimes imposed in the EAG members had a significant impact on AML/CFT supervisory activities. In a number of the EAG member states in the first half of 2020, scheduled inspections in a number of sectors of financial institutions were canceled and on-site inspections were replaced with remote ones.

Supervisory authorities made extensive use of IT tools, such as online verification systems and video conferencing. In the Republic of India, for example, AML/CFT supervision of banks was suspended due to the COVID-19 pandemic outbreak, which was followed by restrictions imposed in March 2020. External analysis of information obtained through data templates of supervisory authorities covering CDD/AML/CFT policies, risk categorization, transaction data, correspondent relationships, incoming and outgoing remittances, transaction mode, account types, etc. was used to monitor banks' activities. Such data templates will allow categorization of risks of specific financial institutions.

In the EAG members, inspections were resumed when the pandemic was largely brought under control. Most EAG member states imposed a moratorium for a certain period of time on the prosecution of financial institutions for minor AML/CFT violations (Tajikistan, Russia, etc.).

Changes in priorities and focus on supervisory activities in the AML/CFT sphere, taking into account the risk-based approach, have become characteristic of a number of the EAG member states.

- In this regard, taking into account the fast growth of the E-commerce segment during the pandemic, the National Bank of Tajikistan when working with bank payment cards and e-wallets pays special attention to the procedures of customer identification, compliance with transaction limits for identified and unidentified customers and providing appropriate reporting. Besides that, the Republic of Tajikistan conducts a sectoral risk assessment in order to improve the effectiveness of the risk-based approach.
- The People's Republic of China has identified countering misconduct related to COVID-19 and potential ML/TF risks, cybercrime and fraud as priorities for AML/CFT supervisory activities.
- The Republic of India has identified as a priority for AML/CFT supervisory activities the need to develop tools for collecting information on the activities of financial institutions, including the development of specific data templates. Besides that, India has emphasized the need for ongoing communication with the private sector.

Engaging in continuous and effective dialogue with institutions allows supervisors to identify the real difficulties faced by reporting entities and apply

corrective measures/sanctions only in noteworthy cases. This will increase the effectiveness of supervisory measures. India identified operations on accounts opened during the pandemic as areas of increased attention, as well as cross-border operations, etc.

The practice of the Russian Federation to collect information on ML/TF risks and vulnerabilities observed by reporting entities through the functionality of the Personal Account on the Rosfinmonitoring website is interesting.

Rosfinmonitoring developed special questionnaires for various sectors of reporting entities with questions that involve selecting one answer out of several or assessing the significance of a phenomenon (trend, risk) using a 5-point scale. Subsequently, a special software module allows to aggregate information and identify the most common answers and average values of assessments.

For example, a survey of more than 400 real estate agents revealed the specific risks of real estate transactions, as well as threats and vulnerabilities in the sector in the context of the spread of COVID-19.

In most of the EAG member states, the staff of AML/CFT departments of financial institutions started to work remotely.

External restrictions in the context of the pandemic prompted competent authorities to more quickly organize the regulation of remote identification of clients. The National Bank of Tajikistan developed and implemented rules and procedures for remote identification for customers of financial institutions that signed an offer agreement for the use of e-wallets.

Financial institutions changed their operating environments to accommodate external constraints. In a number of countries, financial institutions introduced new products and procedures that are almost entirely based on virtual platforms.

Banks in EAG members are generally required to have a business continuity planning policy approved by the Board (Board of Directors), which, among other things, covers recommended actions during crisis situations, such as a pandemic outbreak. Besides that, in most countries, national banks and other financial institution supervisors have informed reporting entities about the business continuity ensuring measures, including the establishment of a rapid response team, which will provide regular updates to senior management on significant events and act as a single point of contact with regulators/external institutions/agencies.

In a number of countries, financial institutions established a crisis response team and a COVID crisis management committee. Normal customer due diligence procedures have been suspended due to quarantine and restrictive measures.

Recommendation:

Competent authorities of the EAG members are invited to consider expanding the use of IT tools for remote interaction with reporting entities:

- for conducting non-contact supervision,

- for prompt collection of information on risks and vulnerabilities among a wide range of respondents.

Summary of recommendations following the results of the study:

Analyze the practices of financial institutions in applying the right to refuse to conduct transactions and the right to refuse to enter into an account (deposit) agreement as risk mitigation measures applied by financial institutions and, if necessary, take measures to optimize them (guide financial institutions towards more active application of barrier measures to reduce ML/TF risks, prepare guidelines and recommendations for financial institutions and entrepreneurs).

Consider the feasibility of keeping records in various statistical excerpts of the amount of information on refusals to provide services to a customer by reporting entities and the volume characteristics of transactions in respect of which they have been applied. The information can be used for trend analysis, national and sectoral risk assessments and other analytical purposes.

Consider including in the format of the electronic message about a suspicious transaction information about the customer's beneficial owner, as well as the IP and Mac addresses of the devices used by customers in remote banking, as well as a special marking to highlight important STRs that require an urgent response.

The countries that have not passed mutual evaluations should assess the feasibility of amending their AML/CFT legislation to properly implement the FATF Standards for identifying and reporting suspicious transactions to FIUs (Recommendations 20 and 10), including:

- introducing provisions that would allow the financial institution to believe that the implementation of CDD measures will alert the client when there is suspicion of ML or FT, and to file a STR instead of conducting CDD;
- submitting STRs not only on actually performed transactions, but also in case of attempts to conduct transactions.

Consider the feasibility of developing financial profiles of criminals for the main predicate crimes (risk areas) identified during the NRA (e.g., "Drug Trafficker", "Corrupt Official", etc.), including transactional and behavioral indicators that allow financial institutions to effectively identify suspicious transactions;

Consider the feasibility of developing (supplementing) a methodology for financial institutions to assess their own risks and vulnerabilities, including analysis of the flow of STRs and reports on refusals to provide services to a customer;

Consider the feasibility of generating reports based on the results of the above assessment and sending them to competent authorities for analysis of ML/TF trends, as well as for use in national and sectoral risk assessments.

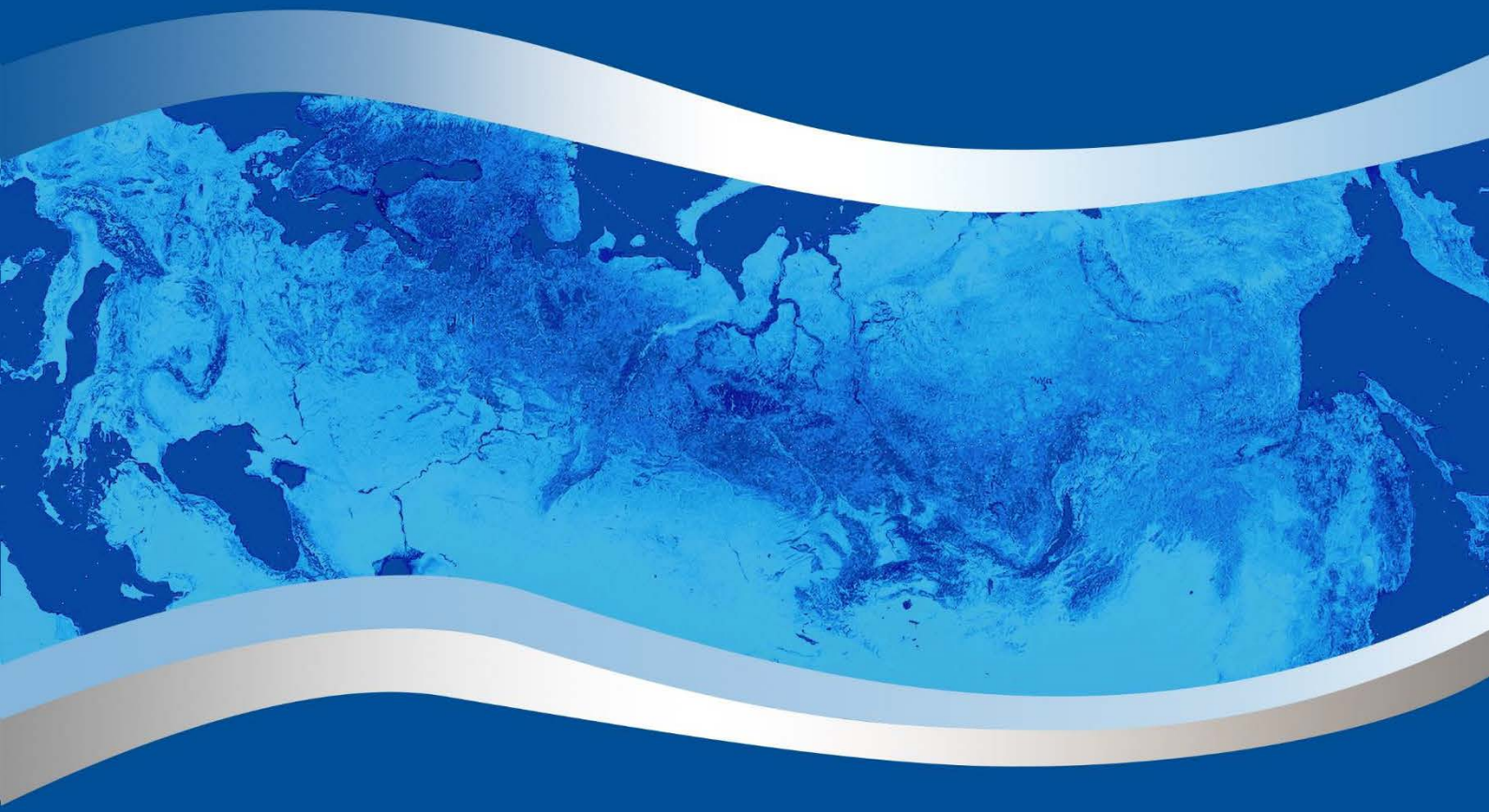
Consider the possibility of expanding the formats of feedback provided, including through:

- the use of automated solutions and Regtech platforms for these purposes;
- developing the public-private partnership formats;
- systematization of work on identifying new ML/TF typologies and promptly communicating them to the private sector;
- targeted cooperation with major financial institutions.

Competent authorities of the EAG members are invited to review, in collaboration with the private sector, current pandemic trends and risks and, if necessary, to update relevant recommendations and guidance documents on identifying high-risk transactions.

Competent authorities of the EAG members are invited to consider expanding the formats of using IT tools for remote interaction with reporting entities:

- for implementation of non-contact supervision,
- for prompt collection of information about risks and vulnerabilities among a wide range of respondents.



www.eurasiangroup.org