

REPORT STRUCTURE
Republic of Kazakhstan
on national risk assessment of legalization
(laundering) of criminal proceeds.

List of abbreviations	2
Conceptual apparatus	3
Introduction	4
Chapter I. Legislative regulation and activities of state bodies in the field of anti-money laundering and combating the financing of terrorism	5
Chapter II. Identification of national money laundering threats, measures taken and planned to minimize risks	7
Chapter III. Identification of national money laundering vulnerabilities, measures taken and planned to minimize risks	22
Chapter IV. Conclusion (summary) on money laundering risks	38

LIST OF ABBREVIATIONS

- **ARDFM** - Agency for Regulation and Development of the Financial Market of the Republic of Kazakhstan.
- **FMA** - Financial Monitoring Agency of the Republic of Kazakhstan
- **STBs** - Second-tier banks.
- **AML/CFT Law** - Law of the Republic of Kazakhstan "On Combating Money Laundering and Terrorist Financing".
- **EAG** - Eurasian Group on Combating Money Laundering and Financing of Terrorism.
- **IS** - Information System.
- **SRC** - State Revenue Committee of the Ministry of Finance of the Republic of Kazakhstan.
- **CHLEU CHCS CIS** - Committee of the Heads of Law Enforcement Units of the Council of the Heads of Customs Services of the CIS Member States.
- **AIFC** - Astana International Financial Centre.
- **MIA** - Ministry of Internal Affairs of the Republic of Kazakhstan.
- **MFO** - Organization engaged in microfinance activities.
- **National Bank** - National Bank of the Republic of Kazakhstan.
- **ML** - Money Laundering
- **OPM** - Operational and Preventive Measure.
- **PO** - Public Official.
- **AML/CFT** - Combating Money Laundering and Terrorist Financing.
- **SFM** - Subjects of Financial Monitoring.
- **FATF** - Financial Action Task Force on Money Laundering.
- **EI** - Electronic Invoices.

CONCEPTUAL APPARATUS

National anti-money laundering system	<p>The totality of state, law enforcement and special bodies of the Republic of Kazakhstan that implement the state policy in the sphere of combating legalization (laundering) of criminal proceeds in interaction and interrelation with the subjects of financial monitoring.</p>
National laundering assessment	<p>Activities of all participants of the national anti-money laundering system, with the participation of financial monitoring entities, to identify threats and vulnerabilities that arise from money laundering, and to develop measures to minimize them.</p>
Threat of money laundering	<p>A person or entity and their actions that may cause danger, loss or damage. In the context of money laundering, this includes criminals, their associates, finances, and other opportunities. A threat assessment typically seeks to identify the amount of income generated by the offences and predicate offences as well as the methods and techniques used to launder the money.</p>
Vulnerability to money laundering	<p>An intrinsic property of a system or structure (including weaknesses in systems or controls, features of financial products and services) that opens up opportunities for abuse or exploitation for money laundering purposes or creates an attractive target for money laundering. Vulnerability assessments focus primarily on risks that allow for the possibility of money laundering.</p>
Risk of money laundering	<p>The potential for harm to the financial system and the economy as a whole through financial transactions for money laundering purposes, due to the realization of the threat and/or the existence of vulnerabilities.</p>

INTRODUCTION

In order to establish the risks and threats to the anti-money laundering system of the Republic of Kazakhstan, a national ML risk assessment was carried out.

This document is the public version of the national ML risk assessment report.

The results of the assessment are to be communicated to all AML/CFT stakeholders (government, law enforcement and the private sector) for practical use (the report is posted on the official FMA website).

The objectives of the national ML risk assessment are:

- identification of frequently used ML schemes;
- identifying vulnerabilities in the financial and non-financial sectors as well as existing legislation;
- developing a common understanding of risks at the national level among the SFM, government, law enforcement and specialized agencies;
- developing measures to minimize and manage ML risks.

In order to achieve the objectives of this study, **the objectives of** the national risk assessment were defined:

- identifying threats and vulnerabilities to ML from predicate and high-risk crimes;
- study of AML/CFT law enforcement practices by state authorities;
- analysis of the criminogenic situation to identify the causes and conditions conducive to ML;
- developing comprehensive AML/CFT measures in the Republic of Kazakhstan.



CHAPTER I. Legislative regulation and activities of state authorities in the field of anti-money laundering and combating the financing of terrorism

Since 2018 (since the first risk assessment), the AML/CFT sphere in the Republic of Kazakhstan has undergone significant changes.

Based on the analysis conducted by AML/CFT experts, the results of the previous assessment were revised and some reforms were implemented to minimize the identified AML/CFT risks and improve the effectiveness of financial intelligence, supervising law enforcement agencies.

In order to ensure compliance of national legislation with the FATF standards in 2020 the Law of the Republic of Kazakhstan "On amendments and additions to certain legislative acts of the Republic of Kazakhstan on countering the legalization (laundering) of criminal proceeds from crime and the financing of terrorism" (№ 325-VI of May 13, 2020) was adopted, which came into force on November 15, 2020.

The main innovations of the law are outlined below:

1) FMA is identified as the regulator for four types of SFM (realtors, lawyers, leasing, accounting organizations and professional accountants; implementation of FATF Recommendation 28);

2) the liability of all SFM for failure to comply with the requirements of the AML/CFT Law (implementation of the FATF Recommendation 35) has been strengthened;

3) provides for the application of targeted financial sanctions for proliferation of weapons of mass destruction (implementation of FATF Recommendation 7) to be applied by SFM and state authorities;

4) mechanism for coordinating risk assessment measures has been established through an inter-agency AML/CFT council (implementation of the 1st and 2nd FATF Recommendations);

5) introduced a risk-based approach in the implementation of SFM inspections (implementation of FATF Recommendation 26);

6) public authority responsible for recording and managing confiscated property and establishing a fund for such property has been identified (implementation of FATF Recommendation 4);

7) strengthened international cooperation in terms of AML/CFT information exchange between financial control and law enforcement authorities and foreign competent authorities (implementation of the 40th FATF Recommendation).

In addition, other amendments and additions have been made to the legal acts to improve AML/CFT activities.

The Anti-Corruption Agency of the Republic of Kazakhstan has adopted three packages of anti-corruption legislative measures aimed at preventing corruption offences and tightening accountability (norms on the dismissal of top managers for corruption among subordinates, a ban for civil servants to hold bank accounts in foreign jurisdictions, an expanded list of subjects of corruption, etc.).

The Interior Ministry has opened a center for combating cybercrime, which has managed to block more than **40,000** messengers and websites with illegal content.

In order to encourage non-cash transactions, the National Bank adopted a resolution to this effect (No. 50 of 21 April 2020; "On limits on the amounts of cash withdrawals by legal entities from bank accounts during a calendar month and categories of legal entities not subject to the requirement to withdraw cash from bank accounts").

Comprehensive measures are being taken to minimize the threats and vulnerabilities of the national anti-money laundering system. Work continues on the implementation of the requirements of the FATF international standards into the legislative acts of the Republic of Kazakhstan.

An institutional and legislative framework for effective interaction with national financial monitoring system participants is in place.

AML Index of the Basel Institute of Public Administration (Basel AML Index), awarded in 2020, is a positive outcome of all this work.

According to the report, which is prepared annually on the basis of official open data and expert opinions, the Republic of Kazakhstan has occupied **73rd place** among 141 countries, having improved its rating in the global AML/CFT index by **45 positions compared** to the previous year (from 28 to 73).



CHAPTER II. Identification of national money laundering threats, measures taken and planned to minimize risks

The following sources of information were used to establish threats and vulnerabilities to the national anti-money laundering system:

- policy and strategy documents, departmental plans of state, law enforcement and special agencies;
- criminal justice statistics of law enforcement and special agencies;
- normative rulings of the Supreme Court of the Republic of Kazakhstan regulating issues of judicial and investigative practice in criminal cases;
- judgments of regional, city and equivalent courts in criminal cases;
- official websites of public authorities;
- the media and Internet resources;
- the records of financial investigations and completed criminal cases;
- reporting of threshold and suspicious transactions subject to financial monitoring;
- information on inspections carried out in relation to the SFM.

Analysis of the criminogenic situation has shown that in recent years there has been a significant reduction in recorded crime of **45%** (from 292,300 in 2018 to 163,200 in 2020).

This was made possible by the coordinated work of law enforcement agencies, as well as the adoption of comprehensive legislative and preventive measures by the state apparatus.

However, there are still potential risks and threats to ML.

The analysis identifies predicate and high-risk crimes.

The following criteria were used in determining them:

- 1) the amount of damage, as well as the proceeds of criminal activity under registered criminal offenses
- 2) crimes committed by an organized criminal group;
- 3) criminal offences for which the criminal proceeds have subsequently been laundered.

The most exposed to threats are ML:

- tax crimes;

- illegal economic activity;
- corruption and embezzlement of public funds;
- fraud;
- drug trafficking.

Tax crimes (fictitious invoicing, tax and customs evasion, economic smuggling)

According to the **Paying Taxes 2020** study by the World Bank and PricewaterhouseCoopers, Kazakhstan ranked 64th out of 190 countries in terms of the way it administers and collects taxes.

In spite of the favourable conditions for entrepreneurship created by the state, some taxpayers resort to various "grey" schemes in order to evade taxes.

Fictitious invoices are one of the main methods **of tax evasion**.

In addition, stolen budget funds are diverted into the shadow through "cash-in-transit" companies.

To a large extent, these crimes are committed as part of an organized criminal group, causing significant damage to the state.

For reference: In 1,033 cases involving fictitious invoices, the loss was 138.1 billion tenge, an average of 133.7 million tenge per offence.

For tax evasion in 533 cases, the damage was 226.3 billion tenge, an average of 424.6 million tenge per offence.

However, a third of all recorded criminal cases related to ML are precisely related to fictitious invoicing and tax evasion.

Economic smuggling causes substantial damage to the economic interests of the state, and significant amounts of customs duties are not paid to the budget.

For information: **24.4 billion tenge** worth of goods were seized in smuggling cases (Article 234 of the Criminal Code) and almost **10 billion tenge** in completed criminal cases involving evasion of customs duties (Article 236 of the Criminal Code).

Although no ML incidents of smuggling were registered during the analyzed period, there are potential threats.

Criminals make huge profits illegally, which are then legalized by setting up and expanding businesses and acquiring movable and immovable property.

In some cases, smuggling is carried out with the assistance of state officials for illicit reward. The proceeds of corruption are also laundered.

Measures taken to minimize the risks.

In the second half of 2019, government agencies have stepped up efforts to reduce criminal "cash-out".

FMA and SRC joined forces and developed common risk management system approaches. Data on potential criminal groups involved in fictitious invoicing has been analytically generated for criminal prosecution and preventive measures (deregistration for VAT, invalidation of registrations and transactions, blocking of electronic invoices, etc.).

Joint work has been organized with the STB, appropriate typologies have been developed, and reporting of companies with signs of a false enterprise has been introduced for appropriate control measures.

In January 2020, a Regulatory Resolution of the Supreme Court of the Republic of Kazakhstan "On certain issues of application by courts of legislation on criminal offences in the sphere of economic activity" was adopted, which allowed systematization of work to counteract false enterprises.

As a result, the detection of **fictitious invoices** has increased by half (from 269 in 2019 to 417 in 2020) and the ending of criminal cases has almost doubled, from **30%** to **57%** (393 out of 693 cases in 2020, 118 out of 396 cases in 2019).

87 criminal groups involved in criminal money laundering and issuing fictitious invoices were suppressed. Criminal cases against **51** groups have been concluded.

For the first time in **five years**, these measures have reduced the level of cash-in-transfer by **38%** (from 2.5 trillion tenge to 1.5 trillion tenge).

Extensive work has been done to improve tax administration.

From 1 January 2020, businesses will switch to the use of online cash registers with data capture and transmission functions across the board.

A voluntary three-part system (online cash register, POS terminal, ERP system) was introduced for individual entrepreneurs, which has had a multiplier effect in terms of reducing shadow cash circulation, increasing business transparency and enhancing tax collection efficiency.

The list of goods required to be entered into the "Virtual Warehouse" module of the Electronic Invoice Information System (EI IS) was expanded, making it possible to track the movement of goods from the border to the end consumer and effectively preventing smuggling, non-commodity transactions and fictitious invoicing.

A project is underway to use IT tools to identify at-risk companies at an early stage and restrict them from issuing ESFs.

As a result of the measures taken, about **6,000** high-risk taxpayers were identified. The additional amount of taxes paid after notices were sent was **16 billion tenge**.

Effective measures have been taken to improve customs procedures, contributing to the prevention of offences.

On 1 January 2018, the new Customs Code of the Eurasian Economic Union and the Code of the Republic of Kazakhstan "On customs regulation" came into force, providing a legal basis for the widespread use of modern information technologies.

The Astana-1 system has been introduced, which has made it possible to transfer customs declarations to an electronic format, simplifying the customs clearance process and minimizing corruption risks.

To reduce grey imports from China, where a significant share of smuggling comes from, a Protocol on electronic exchange of information from online export customs declarations has been signed and **4,900** value-based risk indicators have been introduced.

As a result, the divergence of foreign trade statistics with China fell from **60%** (2017: USD 6.9 billion) **to 40%** (2020: USD 5.3 billion) in 2020.

Planned measures to minimize risks.

In order to prevent fictitious invoices and tax evasion, it is planned:

- Create a single database for all SFM (similar to the "Credit History Data" in the First Credit Bureau) with an accumulation of information on individuals and companies with risk characteristics (including refusal to carry out a transaction, establishing and terminating a business relationship);
 - Upgrade the EI IS in terms of identifying and prohibiting the issuance of EI, and expand the list of goods whose purchase and sale should be reflected in the Virtual Warehouse module;
 - Explore the possibility of additional identification, along with EDS, via Face ID when submitting tax returns and issuing electronic invoices;
 - to develop new **typologies**, to improve **the criteria for suspicious transactions for the SFM** by making additions to the "Rules for submission by subjects of financial monitoring of data and information on transactions subject to financial monitoring and signs of suspicious transaction definition".

In order to prevent smuggling and evasion of customs duties, it is planned to

- Integrate Astana-1, Single Window and the Single Register of Conformity Certificates of the Eurasian Economic Union to automate certificate authentication during customs clearance of goods (will eliminate the possibility of forged certificates being submitted to customs);
 - Automate the exchange of pre-declaration information on goods with China and Uzbekistan (to eliminate the possibility of inaccurate declarations and falsification of shipping documents at the border);
 - Establish online pre-information agreements with the countries most at risk of smuggling (Turkey, Iran, Tajikistan, Turkmenistan, etc.)

These measures will significantly reduce shadow turnover and increase the collection of customs duties and taxes to the budget.

Illegal economic activities (illegal business activities, shadow turnover of oil and oil products, illegal gambling)

The World Bank's Doing Business 2020 ranking places Kazakhstan for the first time in the top 25 countries in terms of **ease of doing business**, improving its position by **11 points** and leaving behind Austria, Spain and the Netherlands (among the evaluated criteria are ease of business registration and customs procedures, "friendliness" of the tax system, etc.).

However, illegal entrepreneurship has not been completely eradicated.

The main reason is the desire of citizens to systematically make profits without complying with legal procedures (the registration process, its labour and cost, time costs, ignoring healthy competition, failure to meet product requirements and standards, etc.), and the increased demand for low-value excisable products.

These offences generate significant profits, which are then legalized.

There is evidence of the registration of criminal cases under ML.

For reference: the amount of damage for crimes related to illegal entrepreneurship for 2018-2020 was **12.1 billion tenge**, with an average of **102.8 million tenge** per crime.

Thus, according to national legislation, **gambling business** should be carried out only in specially designated areas (Burabai in Akmola oblast and Kapchagai in Almaty oblast).

However, unscrupulous individuals, in order to obtain easy profits, organize clandestine casinos, slot machines and gambling terminals. Internet casinos, for which no license is issued in Kazakhstan, are illegal.

For information: the illegal activities of more than **1,700** gambling establishments were suppressed; more than **25,000** gambling items and over **250 million tenge** in cash were seized from circulation. Approximate revenues from the shadow gambling business amounted to **7.4 billion tenge**.

Organized criminal groups (OCG) are often set up to organize gambling, and betting shops and betting shops are used to transfer shadow profits abroad.

In the last 3 years, **10 OCGs** have been dismantled in this area.

For this category of crime, the ML incidence is **16%**.

Illicit trafficking in oil and petroleum products causes multibillion-dollar damage to the country's economic interests.

According to judicial and investigative practice, the criminal proceeds from these crimes are legalized through the acquisition of movable and immovable property.

Trafficking in oil and petroleum products also accounts for **16%** of the total number of criminal cases related to ML.

Measures taken to minimize risks

The downward trend in this type of offence (from 54 cases in 2018 to 35 cases in 2020) is a comprehensive result that includes legislative and preventive measures to reduce the activities subject to licensing, creating conditions for the self-employed to come out of the shadows (trading on social networks, renting, taxi services, etc.).

An internet screening procedure (IBM i2 IS Risk Management System (RMS)) has been automated to identify those carrying out e-commerce activities without registration.

A procedure for cooperation between the SRC and the Ministry of the Interior has been approved for detecting instances of leasing real estate without paying tax.

Work is being done with operators (taxi fleets) on the timely registration of persons carrying out taxi activities through Yandex.Taxi Corp, InDriver, Bolt and other applications.

For information: **892** more people engaged in e-commerce, property rental services and transport services have been registered as individual entrepreneurs.

To combat the illicit production and trafficking of alcoholic beverages, account identification devices (such as the Wipon mobile app) have been introduced that can be used by shopkeepers and consumers to identify illegal alcoholic beverages by scanning the excise stamps.

To eradicate the **illegal gambling business**, the FMA has conducted large-scale operational and preventive measures (OPM), which have resulted in a **40%** reduction in the number of crimes (from 320 to 192) in 2020.

The owners of the commercial premises where the gambling machines were operating illegally were served notices explaining the consequences of criminal

prosecution.

As a result of the monitoring of internet resources by authorized state agencies, **143** websites broadcasting online casinos and other games of chance have been blocked.

The FMA develops new typologies, which are communicated to the SFM for AML/CFT responses.

In the area of combating **illegal trafficking in oil and petroleum products, the Barrel** OPMs are being conducted.

Information systems and IT tools are analyzed to identify the sale of illegal fuels and lubricants, and potential criminal groups in this area are identified.

For reference: **143,000 tonnes** of shadow fuel, worth **24 billion tenge**, were sold in the four groups alone.

The measures taken have resulted in a **2.5-fold** decrease in the number of recorded offences related to illegal trafficking in petroleum products (from 126 in 2018 to 45 in 2020).

Planned measures to minimize risks

The question of introducing registration on the E-gov portal for certain types of business activities is being considered.

An electronic platform "Rental Housing Service" is to be created in order to bring the people who rent out their homes without paying taxes out of the shadows.

In order to reduce the shadow turnover of oil products, it is planned to modernise the "Taxpayer's office" by prohibiting the issuing of accompanying invoices when no goods have been received (except for producers and importers).

Information systems of FMA and the Ministry of Energy of the Republic of Kazakhstan will be integrated for remote monitoring of oil and oil products production and shipment.

This will facilitate the suppression of shady transactions in petroleum products at an early stage.

Through the Cyber Shield of Kazakhstan information system, it is planned to counteract online casinos.

In order to bring illegal gambling out of the shadows of the payment market, the following measures are proposed, based on Russia's experience:

- Enable the competent authority to block websites that are used to transfer money to online casinos without a court order. This would require a list of foreign payment service providers that operate in the gambling industry to be compiled and constantly updated;

Corruption and misappropriation of public funds (corruption offenses and offenses related to the embezzlement of budgetary funds)

The areas, most prone to corruption, remain education, construction, housing and utilities, healthcare and agriculture.

The state allocates large sums of money to finance state programmes and national projects related to economic development, health care, education, employment, social stability in society and the construction of major social facilities.

For information: on the facts of theft 103.2 thousand criminal offenses were recorded, the amount of damage amounted to 1.8 trillion tenge, an average of one crime - 17.4 million tenge.

Fake companies are used to launder the proceeds of this category of crime, through which funds are cashed out or moved abroad.

The main subjects of money laundering from corruption and budget theft are movable and immovable property, the opening of bank accounts, including overseas, and the involvement of money in legal financial and economic activities.

Kazakhstan is taking systematic measures that are yielding positive results.

In the **Transparency International** Corruption Perceptions Index (CPI) for 2020, for example, Kazakhstan moved up **19** places to **94th** place, with a score of 38 for the first time.

Measures taken to minimize risks

The FMA and the Anti-Corruption Agency of the Republic of Kazakhstan for Counteracting Corruption monitor the targeted use of budgetary funds in the placement and implementation of public contracts.

In order to prevent the embezzlement of budgetary funds during the construction of major social facilities, **the Treasury Support** Project has been implemented.

Under it, the general contractor, when selecting subcontractors, ascertains through the state revenue authorities their **trustworthiness** according to set criteria (tax burden, payroll, absence of assets, connection with false enterprises and risky companies).

For reference: **388** infrastructure projects worth **KZT1.9 trillion** are covered by treasury support.

As part of digitalization, a One-Stop-Shop procurement portal has been introduced to ensure transparency and accessibility of the procurement market.

An electronic database of potential suppliers, the E-Depository, has been launched, containing information in the construction sector for the last 10 years.

For reference: The measures taken in 2020 have reduced the number of crimes of embezzlement of budgetary funds by 31% compared to 2018 (from 1,657 to 1,142).

In order to improve control over the illicit enrichment of individuals (including civil servants, their relatives and affiliated persons), Kazakhstan has launched a phased (2021-2025) universal declaration of income and property.

Planned measures to minimize risks

In order to effectively screen high-risk customers, the AML/CFT Law will be amended to introduce a list of positions related to national POs.

Guidelines for realtors and notaries are planned in order to identify illegal transactions for the acquisition and disposal of real estate by POs (with funds obtained through corruption offences).

There are plans to integrate FMA's unified information and analytical system with E-kyzmet, the personnel management information system of the Civil Service Agency of Kazakhstan, to identify suspicious and threshold transactions by POs and other civil servants (winning or losing at gambling houses, foreign currency exchange, overseas money transfers, purchase of expensive property or purchase of property at an unreasonably low price, etc.).

An additional feature of the definition of a suspicious transaction "receipt (payment) of large sums of money from a gambling establishment as winnings from gambling and/or betting on gambling" is being developed, which involves informing financial intelligence, where it is suspected that the customer's activities are related to the performance of public functions.

New **criteria for suspicious transactions** will be developed for transactions related to the acquisition of immovable property, including abroad, as well as for transactions with indications of embezzlement of budgetary funds **for the SFM**, by supplementing the "Rules for submission by subjects of financial monitoring of data and information on transactions subject to financial monitoring and indications of definition of a suspicious transaction".

There are plans to improve the national budget expenditure control system by introducing a "**bank tracking**" project that will track the movement of funds through the entire chain of providers of goods, works and services, regardless of level.

The implementation of this project will be an effective tool in combating the embezzlement of public funds and will ensure transparency of payments.

Fraud (including pyramid schemes)

More than **95,000** crimes in this category have been recorded in the last **3 years** (2018 - 29,282, 2019 - 32,286, 2020 - 33,759).

There has been an annual increase. The proportion of these crimes remains quite high (17-20%) and ranks second after theft.

Fraudsters caused nearly **356 billion tenge** in damages, including **37.6 billion tenge** to the state and **318.3 billion tenge** to individuals and legal entities.

There are many ways to commit fraud. These include: using payment cards, making fictitious loans, setting up and running a pyramid scheme, and others.

Against the backdrop of increased remote shopping and online services, there has been a **twofold** increase in online frauds (from 7,769 in 2018 to 14,220 in 2020).

Criminals use online ad platforms (OLX, Kolesa.kz, Krisha.kz), a banking application (Kaspi.kz) and microfinance organizations.

Using these online platforms, fictitious advertisements are created and the price of the goods offered is significantly reduced, thereby enticing future victims in the form of gullible buyers.

The problem is compounded by the use by criminals of subscriber numbers located in other states.

Almost a third (2,822) of the remaining unsolved Internet frauds in 2020 were committed from post-Soviet states.

There are cases where Kazakh nationals are complicit in such crimes and where Kazakh bank accounts are used as transit points.

As for **pyramid schemes**, they are particularly active in times of financial instability (during financial crises).

In 2020, there was a definite increase in the number of crimes related to pyramid schemes (7.5 times, from 24 to 181, with losses increasing from 360 million to 10.8 billion tenge).

This situation is due to the economic downturn associated with the global pandemic and, consequently, an increase in fraudsters.

The schemes that are used to raise funds from citizens are to some extent controlled from abroad. The possibilities of the information and telecommunication network of the Internet are used, making it possible, on the one hand, to reach directly to the consumer of the "services" and, on the other hand, to make it more difficult to control them.

Few cases of fraud have been reported in relation to ML.

Measures taken to minimize risks

Law enforcement agencies are taking comprehensive measures to prevent emerging threats from fraudulent activities.

Investigative teams have been set up to solve and investigate criminal cases involving crimes committed through the use of information technology.

At the legislative level, the obligation of owners of electronic trading platforms to prevent illegal trade has been established (Article 33-1(1) of the Law of the Republic of Kazakhstan "On protection of consumer rights").

The ARDFM has set up an inter-agency working group on countering pyramid schemes, which is working on preventive and proactive measures to counter pyramid schemes.

The Ministry of Information and Social Development has developed a system called "Automated Monitoring of the National Information Space", which aims to identify and record materials containing signs of pyramid schemes in a timely manner.

The FMA, the ARDFM, the National Bank and the SFM have adopted a roadmap to improve the effectiveness of cooperation on AML/CFT issues. The roadmap provides for a procedure for compiling and exchanging lists of companies whose activities are suspected of being pyramid schemes.

A large-scale public awareness campaign has been organized and materials on the signs and consequences of fraud are published. ARRF has launched a telegram channel and a mobile application, Fingramota Online, where advice is provided in response to questions from the public.

Planned measures to minimize risks

The Ministry of Internal Affairs has a planned departmental programme to combat crimes in the field of information and communication.

It will organize anti-fraud collaboration with government agencies, financial institutions, mobile phone operators, service providers and online platforms.

In order to suppress pyramid schemes at an early stage, it is planned to

- create a unified register of organizations that have signs of financial (investment) pyramid schemes and make it available on official internet resources accessible to the public;
- extend the aims and objectives of the system "Automated Monitoring of National Information Space" by building an analytical model to identify and capture materials containing signs of pyramid schemes (on websites, social messengers and other mobile applications).

The implementation of these measures will make it possible to effectively combat fraud on the territory of the Republic of Kazakhstan and ensure the financial security of citizens.

Drug trafficking

This section includes offences related to the illicit manufacture, distribution and smuggling of narcotic drugs, psychotropic substances and precursors.

Drug addiction is a major threat to the health and gene pool of the nation, the economy, the rule of law and state security. Therefore, active counteraction to drug-related crimes and effective prevention of drug addiction are the most important tasks of the state and society.

A serious factor continues to be the presence of its own cannabis raw material base in the Chui Valley, from where it feeds plant-based drugs for all regions of Kazakhstan.

For reference: There has been a slight increase of 10%, or 768 cases, in drug trafficking offences in Kazakhstan.

At the same time, large-scale heroin production in Afghanistan continues to pose a serious threat.

Due to its geographical location, Kazakhstan is on the so-called northern route used to traffic heroin to Russia, other CIS countries and the European Union.

According to the CIS Executive Committee, Kazakhstan seized the largest average annual quantity of heroin (391 kg) between 2016 and 2019.

However, according to international analysts as well as Kazakh law enforcement agencies, Afghan heroin trafficking through Kazakhstan is on the decline every year.

Instead, there has been an expansion of the market for synthetic drugs, which do not require plant material for their manufacture.

New forms of illegal activities of organized criminal groups and communities are emerging, and they are strengthening the conspiracy of supply and distribution channels by using innovative communication systems. In some regions, the results of dismantled drug laboratories and clandestine workshops are already available.

In terms of ML schemes, drug trafficking is quite common worldwide as a source of funding for organized crime (including transnational) as well as for terrorist and extremist organizations.

The proceeds are then used to fuel criminal businesses and to purchase

weapons, real estate and expensive vehicles.

In Kazakhstan, the percentage of registered ML cases related to drug offences is just over **7%** of all registered cases in this area.

As a result of this category of predicate offences (under articles 286, 296, 297, 298, 299, 300, 301 and 302 of the Criminal Code of the Republic of Kazakhstan), damage totaled **313.7 million tenge**.

Measures taken to minimize risks

The law enforcement and special agencies of the Republic of Kazakhstan systematically carry out joint operations to suppress the illicit trafficking of narcotic drugs (operations "Poppy", "Channel", "Doping", "Barrier", "Carrier", etc.).

On an annual basis, the Ministry of Internal Affairs conducts Karasora operations in the Chui Valley.

For reference: In 2020, the Karasora operation resulted in the detection of more than **1,750** drug offences and the seizure of more than **22 tonnes** of drugs from the illicit traffic.

There is effective international cooperation in the fight against drug smuggling.

The CHLEU CHCS CIS has established a working group to coordinate cooperation between law enforcement units of CIS member states on countering drug smuggling.

The World Customs Organization's Regional Law Enforcement Liaison Hub for CIS countries RILO-Moscow FMA exchanges proactive information on possible cross-border drug trafficking channels through the CENcomm operational platform channels. A procedure for the exchange of information on drug couriers has been approved.

Every year the FMA takes part in the international special operation "Sentinel" (involving customs and law enforcement agencies of CIS and non-CIS countries) aimed at suppressing cross-border drug trafficking channels.

On the basis of a memorandum of understanding between the FMA and the German Criminal Police, there is effective cooperation in combating cross-border drug trafficking.

Eight joint controlled deliveries were conducted and over **10 kg of** drugs and psychotropic substances (grain marijuana, cocaine, MDMA (Ecstasy) dimethyltryptamine, amphetamine, LSD, mushrooms, etc.) were seized from illegal traffic.

In 2019, FMA officers disrupted **the largest ever** international drug trafficking from Iran to the Netherlands, transiting Kazakhstan. During the operation, heroin with a total weight of **1,104 kg** (worth more than USD 500 million, in doses worth more than USD 1 billion) was seized.

A large-scale international special operation using the "**controlled delivery**" method involving the intelligence services of six countries (Russia, Belarus, Lithuania, Poland, Germany and the Netherlands) was carried out, which resulted in the suppression of a transnational OCG (consisting of citizens of Turkey, Serbia and Germany) engaged in smuggling and selling drugs in the European Union in Andernach (FRG).

In order to respond to the emergence of new psychoactive substances in a

timely manner, the Government is empowered to approve the list of psychotropic substances and determine their "criminal" amounts.

On **5 July 2019**, an updated list of narcotic drugs came into force, including **89** basic structures of synthetic drugs. Taken together, these measures have brought **some 1,000 all known** substances under government control today.

Amendments to the Criminal Code of the Republic of Kazakhstan have been adopted to classify the sale, inducement to use drugs through the Internet and other electronic information resources as a **particularly serious offence**.

All those involved in so-called online shops (from the administrators of such sites to the "bookmarkers" and distributors of graffiti signs) are included in the orbit of criminal prosecution.

A new provision has been introduced in the Criminal Code of the Republic of Kazakhstan (Article 299-1) which criminalizes the promotion and illicit advertisement of drugs.

Planned measures to minimize risks

Financial intelligence units will be used to identify drug trafficking channels as well as ML schemes.

Modern typologies will be exchanged on the EAG platform to focus the attention of law enforcement agencies of EAG member states on high-risk areas and take timely measures to dismantle international drug trafficking channels and financial flows from these criminal activities.

There are plans to work out the issues:

- the legal status, grounds and procedures of transport and logistics companies, as well as interaction with postal organizations, should be established in law;
- developing an additional mechanism for passing identification of e-money users when they are tied to mobile network operators;
- the international cooperation in the fight against cross-border drug trafficking should be intensified.



CHAPTER III. Identification of national money laundering vulnerabilities and measures taken and planned to minimize risks

In order to assess AML/CFT risks, vulnerabilities of the national anti-money laundering system have been identified alongside the threats. These include:

- cash circulation;
- the use of nominee legal entities (shell companies) to run ML schemes;
- transfers abroad of money obtained by criminal means;
- imperfect risk management by public authorities and the financial sector;
- insufficient explanatory work with the subjects of financial monitoring (on AML/CFT legislation, existing risks and threats of money laundering).

In order to identify and categories vulnerabilities in the national anti-money laundering system in the field of ML, appropriate risk criteria are defined:

- the general situation in the financial and non-financial sectors and the volume of transactions taking place;
- information on the implementation of AML/CFT legislation by the SFM;
- availability of information systems and IT tools for the application of due diligence measures;
- the types of services, products, operations provided, taking into account the specific nature of the SFM's activities.



HIGH RISK GROUP FOR MONEY LAUNDERING

Use of STBs and selected banking institutions in ML schemes

The banking sector as a whole is the most regulated and law-abiding in terms of AML/CFT compliance.

The technical equipment of the STB allows for timely identification and action on suspicious customers and transactions.

However, despite this, there are potential ML risks.

Selected high-risk transactions with indications of ML are conducted through banks and organizations, large sums of money are transferred abroad and cashed out from the accounts of nominee legal entities and citizens with low social responsibility, contrary to established typologies, internal controls and technical tools.

Measures taken to minimize risks

The ARDFM has a number of reactive measures in place in relation to STBs and entities engaged in certain types of banking operations.

On an annual basis, an assessment is made of the involvement of STBs in dubious transactions.

Taking a risk-based approach, trends in the banking sector's exposure to ML risks are explored.

The STBs have automated processes for identifying threshold and suspicious transactions using a variety of scenarios, calculating customer risk based on minimum parameters (country risk, customer type, product/service risk).

Online screening of clients against lists of persons and organizations linked to the financing of terrorism and extremism and foreign public officials is conducted (both at the time of establishing a business relationship with the client and when servicing the client).

The list of grounds on which administrative measures may be imposed on SFM in case of non-compliance with AML/CFT legislation was expanded (from 4 to 13).

The ARDFM has developed recommendations and typologies for identifying indicators of ML offences (summarizing the most common indicators of suspicion and developing indicators for detection). They are posted on the National Bank's web portal for use by STBs in monitoring customer transactions and taking appropriate measures

to minimize ML risks.

Use of nominee entities in ML schemes

The risks of using nominee legal entities to carry out illegal financial transactions are quite common. This is evidenced by financial investigations as well as completed criminal cases of fictitious invoicing and tax evasion (accounting for 36% of all ML cases).

Often, the opening of fly-by-night companies will be for people with low social responsibility or those who are unaware of their involvement in the company's activities.

Large flows of financial transactions pass through nominee legal entities, which are monitored and reported to law enforcement and state revenue authorities for timely responses.

The use of non-residents in illicit schemes continues to occur in the presence of legal restrictions on non-residents.

This makes it difficult to identify and prosecute the organizers and those involved.

The use of bank intelligence facilitates a rapid response to risky transactions, the identification of the affiliation of group entities, the identification of each actor's role, and the identification of new members of the criminal group.

For reference: **499** FIU communications sent between 2018 and 2020 were used in the analytical formation of **45** schemes of suspected criminal groups.

Measures taken to minimize risks

In order to prevent vulnerabilities associated with the use of nominee entities in ML schemes, state authorities are taking the following measures:

- STBs use internal control and compliance tools and have organized effective controls over transfers and cash withdrawals;
- AML/CFT rating of the STBs has been approved and quarterly meetings are held with compliance offices at the FMA to discuss results and AML/CFT cooperation issues;
- typology on the characteristics of fictitious invoicing, which defines the types, criteria and patterns of suspicious transactions, has been approved and communicated to the STBs;
- a unified register of persons with risk criteria is available on the closed part of the FMA's website for timely action by the STB to verify its clients and prevent suspicious transactions (these lists are integrated into the BVU's information systems for prompt decision-making);
- tripartite agreement has been concluded between the FMA, the National Bank and the ARDFM, under which the National Bank sends monthly information on the amount of cash disbursed by oblast branches of the STBs;
- from STBs to FMA reports on the turnover of money disbursed by cash settlement units (amendments were made to the resolution of the Board of the National Bank "On Approval of the List, Forms, and Terms of Reporting by STBs");

- Information on false companies is exchanged between the FMA and SRC and measures are taken to neutralize their activities.

Planned measures to minimize risks

In order to prevent vulnerabilities associated with the use of nominee entities in ML schemes, it is planned to

- establish a single database for all SFMs with an accumulation of information on persons and companies with risk indicators (including refusal to carry out a transaction, establishment and termination of business relations), STB to increase the number of information sources and analysis tools;
- ensure that the risk management system of FMA, SRC, STB and the National Chamber of Entrepreneurs of the Republic of Kazakhstan "Atameken" correspond with regard to business entities;
- to amend the AML/CFT Law with regard to recording the information on the visa of a foreigner or stateless person, which is necessary for the identification of a natural person;
- FMA to develop typologies on business immigrant visa verification when conducting SPC on non-residents;
- to update the typologies for detecting fly-by-night companies, with relevant amendments to the Minister of Finance Order No 938 of 30 September 2020, and to communicate them to the STBs for internal control measures to be taken.

The use of gambling and lottery organizers in money laundering schemes

The following types of gambling activities are permitted in Kazakhstan under national law:

- casino;
- arcade;
- bookmaker's office;
- sweepstakes.

The risk of using the gambling sector in ML remains high.

The gambling business could very realistically be used to exploit ML schemes by laundering the proceeds of crime through winnings from casinos, bookmaker's bets and sweepstakes.

This category of SFM is subject to regulation and licensing.

There has been an increase in the work of the single lottery operator, whose activities resulted in a **76%** increase in the number of messages received from it during the reporting period.

Instances of illegal gambling (online casino) activities by betting organizations were detected.

Measures taken to minimize risks

In 2020, the Law of the Republic of Kazakhstan "On Gambling Business" was amended to regulate the placement of betting offices (bookmaker's offices) only in resort

areas (on the coast of the Kapshagai reservoir of Almaty region and in the Burabai district of Akmola region).

At the same time, online casinos are banned in Kazakhstan under this law.

However, there are gambling schemes, including betting shops, bookmakers' offices and online casinos, with questionable turnover (indications of "shadow" income).

For example, in Mangistau region, a bank employee illegally stole more than **90 million tenge** from customer accounts. Later, he cashed out part of the funds through a bookmaker's office.

A number of online casinos, which also operated under the guise of bookmakers, were detected. Criminal proceedings have been instituted against officials of the **PariMatch, VK Triumph, Favorit and PROFITBetting** bookmakers for organizing illegal gambling activities.

There is also extensive work on the part of the FMA to involve the SFM in AML/CFT work.

The Ministry of Culture and Sports of the Republic of Kazakhstan has introduced the practice of preventive control of gambling businesses.

As a result, two violations of AML/CFT legislation were identified. Based on the results of the inspections, orders were issued to rectify the identified violations, which were rectified by the control subjects.

In addition, the above-mentioned authorized state body is working on the implementation of a Rate Recording Centre (RRC), the purpose of which is:

- ensuring transparency in the betting industry;
- automation of AML/CFT procedures;
- blocking channels for money out of the country;
- an independent channel of information to assess and analyze the state of the industry and make timely adjustments;
- 24-hour call center to provide psychological support to problem players and their relatives;
- the widespread introduction of mechanisms to limit and self-restrict participation in betting and wagering.

The Front office platform has been implemented, which provides for new approaches to interaction with the SFM. Its main objective is to provide AML/CFT participants with feedback and customer focus on a one-stop-shop basis.

Typologies on the use of gambling in ML schemes are developed and communicated to the SFM to verify their clients and take appropriate AML/CFT responses.

During the analyzed period, the number of reports from gambling organizers subject to financial monitoring increased by **21%** or **200** transactions.

Use of microfinance institutions (including pawnshops) in **ML schemes**

The fact that MFOs are involved in fraudulent schemes and ML, the lack of automation processes for this category of SFM do not allow them to fulfil their obligations effectively and pose significant ML risks.

The specifics of MFOs are due to their ability to legally raise funds from legal entities and then redistribute them between legal entities and individuals, including issuing nominal (knowingly non-repayable) micro-loans. They are mostly issued to persons who have lost their identity (documents) or who have low social responsibility. The proceeds are legalized in various ways.

Another risk factor was the relatively unsophisticated registration of MFOs, which could initially be exploited for ML schemes by their founders and managers.

However, as a result of legislative changes, from 1 January 2021 a license from an authorized body is required to carry out microfinance activities.

There is a practice of unscrupulous MFOs transforming themselves into pyramid schemes, the main purpose of which is to obtain material benefits through financial fraud.

Their modus operandi are varied (messenger-based cash registers, network marketing, cooperatives, intellectual product services, internet sites with a learning platform, etc.).

For example, in 2020, the activities of certain financial organizations (Garant 24 Lombard LLP, ESTATE Lombard LLP, Vygodny Loan LLP) affected almost **17,000** citizens, causing more than **KZT21 billion** in damage. **Thirty-two** criminal cases were registered in **14** regions of the country.

An analysis of law enforcement activities also indicates that there are instances of perpetrators using pawnshops to take possessions and cash.

Often, these institutions are where the stolen property is sold, which creates additional risks for ML schemes.

Measures taken to minimize risks

The designated government agencies are working together to take comprehensive measures to minimize the risks of using MFOs in ML.

From 1 January 2021, a new version of Article 14 of the Law of the Republic of Kazakhstan "On Microfinance Activities" was enacted, which specifies a number of leverage points for legal entities in their implementation as MFOs.

Background:

- A legal entity registered as an MFO shall, within six months (from the date of its state registration), apply to an authorized body for a license (to carry out microfinance activities);
- A legal entity intending to engage in microcredit activities shall notify the financial monitoring authority of state registration (re-registration) as an MFO within ten calendar days (from the date of such registration).

A number of comprehensive measures, including cooperation with other authorized state bodies, have been taken to curb illegal activities on the part of MFOs.

At the same time, from 1 January 2020 paragraph 3-1 of Article 4 of the Law of the Republic of Kazakhstan "On Microfinance Activity" came into force, which regulates the procedure for determining the annual effective interest rate on microcredits up to 50 MCI, issued for a period of up to **45** days.

To prevent microloans from being issued to front men, the National Bank has approved Rules for granting microloans electronically (National Bank Decision No. 217 of 28 November 2019), which came into force on 1 January 2020.

According to these Rules, before granting a micro-loan electronically, the MFO conducts due diligence on the client in accordance with AML/CFT legislation.

Electronic digital signature, biometric and two-factor authentication are used to identify the customer.

In order to curb the sale of stolen property through pawnshops, the National Bank has approved the Rules for the organization of pawnshop activities, which include measures to counteract the circulation of illegally obtained items in pawnshops, which took effect on 1 January 2020 (National Bank Decision No. 226 of 28 November 2019).

According to this legal act, pawnshops are required to provide information on collateral to the State Credit Bureau JSC. In turn, the Ministry of the Interior monitors this information through access to the State Credit Bureau's database and responds in a timely manner (an agreement was signed on 10 February 2021).

In addition, a trilateral agreement (FMA, ARF, National Bank) was signed on interaction and cooperation in the field of AML/CFT, counterfeiting and currency control (defining the procedure for cooperation in identifying violations of AML/CFT legislation by MFOs).

A roadmap was developed to improve the efficiency of cooperation between the competent authorities (the ARDFM, the National Bank and the FMA) and the SFM on AML/CFT issues. The roadmap provides for a procedure for the formation and exchange of lists of companies whose activities are suspected of being pyramid schemes.

FMA conducts regular outreach to this category of SFMs, and has developed and communicated typologies aimed at identifying patterns and methods of identifying suspicious transactions and customers.

As a result of the work carried out (as of June 1, 2021), the maximum number of microfinance providers has been achieved. Their number was **992** entities, of which **955** have already been registered in the FMA financial transaction data collection system (96% coverage).

Planned measures to minimize risks

In order to systematically improve the regulation of MFOs and pawnshops, there are plans to work with the ARDFM and the National Bank:

- reducing the timeframe for providers to submit information, including information on microloans, to the State Credit Bureau;
- compulsory reorganization or liquidation of MFOs that fail to register;
- introduction of new criteria for suspicious transactions for pawnshops (systematic pawning of movable/ immovable and/or other property without further redemption) by supplementing the "Rules for submission by subjects of financial monitoring of data and information on transactions subject to financial monitoring and indications of suspicious transaction definition";
- Developing and communicating to pawnshops a register of risk takers (who systematically rent movable/ immovable and/or other assets to pawnshops without further

redemption and others) for internal control measures and timely reporting to authorized bodies.



MEDIUM RISK GROUP FOR MONEY LAUNDERING

Use of virtual currencies (cryptocurrencies) in ML schemes

In the Republic of Kazakhstan, the only legal tender is the national currency tenge. Thus, cryptocurrency cannot be used as a means of payment within the country.

The anonymity of cryptocurrency payments ensures the popularity of this payment method in the commission of crimes and makes the investigation process more difficult for law enforcement.

For example, cryptocurrencies can be used as payment for illegal transactions (for drugs, weapons, etc.).

Meanwhile, virtual assets are used in Kazakhstan by AIFC participants that are SFM.

Since its launch in 2018, AIFC, positioning itself as a global center for business and finance in Kazakhstan and Central Asia, has been expanding its legal framework and offering new organizational and legal forms of doing business in Kazakhstan.

FATF Recommendation 15 requires countries to ensure that virtual asset service providers are regulated and licensed (or registered) for AML/CFT purposes, and have effective monitoring systems in place to manage and minimize the risks arising from the circulation of virtual assets.

In this regard, legal regulation of virtual asset service providers is defined in the AIFC area.

Most AIFC participants started their activities in 2019-2020. In this regard, the reason for the inactivity of some of them is the lack of clients.

Therefore, at this stage it is not possible to fully and qualitatively assess the level of ML risks and the effectiveness of their AML/CFT measures.

Measures taken to minimize risks

Law enforcement agencies, as well as financial intelligence, monitor banned sites and monitor cryptocurrency transactions, including legal mechanisms for international cooperation.

Typologies for disrupting ML schemes involving cryptocurrencies are being developed and communicated to the SFM, especially those conducting business

activities in the AIFC.

The EAG is also conducting typological studies to identify cross-border drug settlement schemes involving cryptocurrency.

Data from law enforcement and financial intelligence units of EAG member states on methods of criminal settlement and models of legal regulation of the use of cryptocurrencies are summarized.

AIFC's Financial Services Regulatory Committee conducts an annual thematic review of participant compliance.

In turn, reports include a description of internal control systems, results of customer due diligence measures, client and business risk assessments, rejection and freezing measures, identification of suspicious transactions, sanctions list checks and reporting to the FMS.

Planned measures to minimize risks

The AML/CFT legislation is currently being amended to include persons carrying out business activities with digital assets in accordance with the Law of the Republic of Kazakhstan "On Informatization".

Use of payment organizations in ML schemes

There are **70** payment organizations in the Republic of Kazakhstan.

Every year there is a downward trend in the number of transactions through payment organizations (2018 - 469.3 million transactions, 2019 - 463.1 million transactions, 2020 - 430.1 million transactions).

At the same time, the volume of transactions grows every year (2018 - KZT 1.5 trillion, 2019 - KZT 1.9 trillion, 2020 - KZT 2.3 trillion).

The largest e-money systems are, Qiwi Kazakhstan, Woopay, and Personal Checkout.

This category of SFM is sufficiently regulated at the legislative level and falls under the jurisdiction of the National Bank.

Attracting criminals is the ability to use non-personalized (anonymized) details of remitters and beneficiaries to carry out illegal financial transactions.

There have been cases of electronic means of payment registered in the name of persons unaware of the nature of the use of these instruments, including in ML schemes.

Electronic payments are also used for fraudulent activities, including those originating from other countries.

Measures taken to minimize risks

In 2020, the legislation of the Republic of Kazakhstan was amended to prohibit payments and transfers in favour of unidentified clients of e-money systems, and to prohibit redemption (withdrawal) of e-money by unidentified clients.

Also depending on the status of customer identification were established:

- on the amounts of transactions;
- on the maximum amounts stored in a single e-wallet.

These changes are aimed at reducing ML/TF risks in e-money systems.

This leaves the risks associated with opening a wallet in favour of third parties who are often not involved in organizing criminal schemes.

As a preventive measure, authorized state agencies monitor banned websites and trace e-wallet transfers.

Awareness-raising activities have been organized for payment organizations and recommendations and typologies for the suppression of ML schemes are being developed.

Cash couriers

Pursuant to FATF Recommendation **32**, measures should be taken to detect the cross-border movement of cash and bearer negotiable instruments, including through a declaration system and/or disclosure system.

The current practice of monitoring the movement of money across the customs border is as follows

In accordance with the requirements of customs legislation, individuals may import or export foreign and national currency in cash without a customs declaration, not exceeding the equivalent of **USD 10,000**.

At the airport, a passenger carrying money not subject to declaration undergoes customs control in the "green" corridor (selective inspection).

Due to Kazakhstan's membership of the Customs Union of the Eurasian Economic Union, there is no customs control at the internal border of the member states.

Only border passport and export (customs) controls (for legal entities) are carried out.

These circumstances pose certain threats to the use of individuals crossing borders in the transportation of criminal funds (risks of using cash couriers for ML).

Measures taken to minimize risks

The legislation provides for administrative (Articles 535, 546-551 of the Code of Administrative Offences) and criminal (Article 234 of the Criminal Code of the Republic of Kazakhstan - economic smuggling) offences.

In turn, an analysis of criminal statistics under Article **234** of the Criminal Code of the Republic of Kazakhstan shows sporadic cases of investigations related to the illegal transportation of cash across the border of the Republic of Kazakhstan.

The number of cases involving administrative offences under Article **551** of the Administrative Offences Code of the Republic of Kazakhstan (failure to declare or false declaration of goods, cash, false declaration of information in customs documents, etc.) amounted to **287**.

Planned measures to minimize risks

In order to reduce the risks of cash couriers being used in ML schemes and to enhance the detection of undeclared cash moving through customs and border posts.

The Ministry of Finance of the Republic of Kazakhstan plans to integrate passenger databases with its resources to determine the frequency and purpose of

customs border crossings of both Eurasian Economic Union member states and other border states.

In turn, the FMA plans to develop the following measures as additional measures to detect undeclared cash, monetary instruments or misdeclared cash:

- strengthen analytical work in the framework of existing joint plans with the state revenue authorities, using their resources to obtain information from the competent authorities of other countries on the cash declared by individuals when entering the country;
- organise mutual exchange of information between financial monitoring bodies, customs, border guards and airport security on the movement of cash by individuals across the state border of Kazakhstan;
- to monitor, analyze the route and frequency of movement of natural persons across the border using available information databases;
- actively use the potential of sniffer dogs, specially trained to detect money, when carrying out searches at customs and border posts;
- when carrying out customs and border controls, make extensive use of modern technical means of customs control (X-ray machines, etc.) to detect money concealed from control.

The use of individual entrepreneurs and legal entities providing intermediary services in real estate transactions (hereinafter referred to as realtors), notaries in ML schemes

The judicial and investigative practice in corruption cases shows that the criminal proceeds from bribes and embezzlement of public funds are often invested in real estate.

However, the main ML risks through the real estate sector relate to the investment of capital of dubious origin in commercial and residential properties abroad.

In this case, the risk is due to the lack of transparency of the beneficial ownership structure of properties acquired in foreign jurisdictions.

As a rule, the purchase and sale of real estate is carried out directly with the participation of a notary; realtors in this case act solely as intermediaries between sellers and buyers (providing advice and information support).

Such transactions go through the STBs, which carry out an internal control procedure and request the relevant documents.

After completing the transaction and paying the fee for the property, the title deeds go through another stage (before the registration of property rights) - on the site of the Non-public joint-stock company "State Corporation "Government for Citizens".

It should be noted that the cross-checking of real estate transactions by STBs and notaries effectively prevents ML in this sector.

In the meantime, some of the vulnerabilities of ML schemes in the sector need to be highlighted, which include:

- absence of a state body monitoring the implementation of AML/CFT legislation by real estate agents;
- lack of a unified register of real estate agents in the country due to the imperfection of the general classifier of economic activities;
- registration by law enforcement agencies of real estate brokering services provided by real estate agents to persons who have committed illegal financial transactions.

Measures taken to minimize risks

To a certain extent, the establishment in national legislation of a time limit within which an owner cannot sell an acquired property without paying income tax has reduced the risks of using the property in ML schemes.

FMA is working to further increase the AML/CFT coverage of the real estate sector through the use of the "Remote Monitoring" platform.

Planned measures to minimize risks

In order to take measures to minimize ML risks, it is planned to

- identify an authorized state body to regulate the activities of real estate agents, as well as the licensing of persons providing intermediary services in real estate sale and purchase transactions;
- revise the general classifier of economic activities for real estate agents, including distinguishing between recruitment and sales services (in order to specify the activities of the CPM);
- work on lowering the threshold for transactions involving the purchase and sale of immovable property;
- provide in the requirements of the internal control rules for action to be taken by realtors with regard to all parties to a transaction (seller and buyer).

These measures would strengthen AML/CFT in the real estate services sector.

Use of other SFM in ML schemes (organizations involved in certain types of banking operations and exchange transactions, professional participants in the securities market, central depository, insurance (reinsurance) organizations and brokers, mutual insurance companies, individual entrepreneurs and legal entities carrying out leasing activities without a license, as well as with precious metals and precious stones and jewellery made from them)

The analysis showed the presence of specific vulnerabilities in this category of SFM, in particular:

- absence of a regulatory authority during the period in question;
- Insufficient automation of the monitoring of financial transactions;
- existence of a significant number of detected irregularities, with proper organization of controls by the state authorities.

However, as practice shows, they have not been used in ML schemes in Kazakhstan, i.e. these sectors do not pose high risks to the national anti-money laundering system.

In order to minimize the possible negative impact of vulnerabilities, remedial



measures are being developed.

CHAPTER IV. Conclusion (summary) on money laundering risks

The National Money Laundering Risk Assessment 2018-2020 allowed all participants in the anti-money laundering system to identify the main threats, vulnerabilities and high-risk areas specific to Kazakhstan.

The results have led to measures aimed at reducing ML risks and increasing the effectiveness of the national anti-money laundering system, which include

- improvement of national legislation;
- expansion of departmental plans of state bodies;
- modernization of information exchange and strengthening of human resources capacity.

The report is a practical tool for use in the work of all actors involved in the national AML/CFT system and for consideration in regional and sectoral AML/CFT risk assessment projects.

The government and law enforcement agencies of Kazakhstan are encouraged to refocus their activities on a risk-based approach and the measures outlined in the ML risk minimization plan. This will increase the effectiveness of financial investigations, ensure confiscation measures and asset recovery.

Regulators have been encouraged to engage more effectively with the FMA in relation to the development of guidance manuals for the SFM as well as sectoral risk assessments.

The SFM is recommended to use the results of the national risk assessment in its operations to modernize its internal control regulations in terms of categorizing its services, products, and customers in the light of the ML risks identified and taking effective mitigating measures.