



EAG



MEETING OF THE INTERNATIONAL  
COMPLIANCE COUNCIL

COLLECTION OF PRESENTATIONS

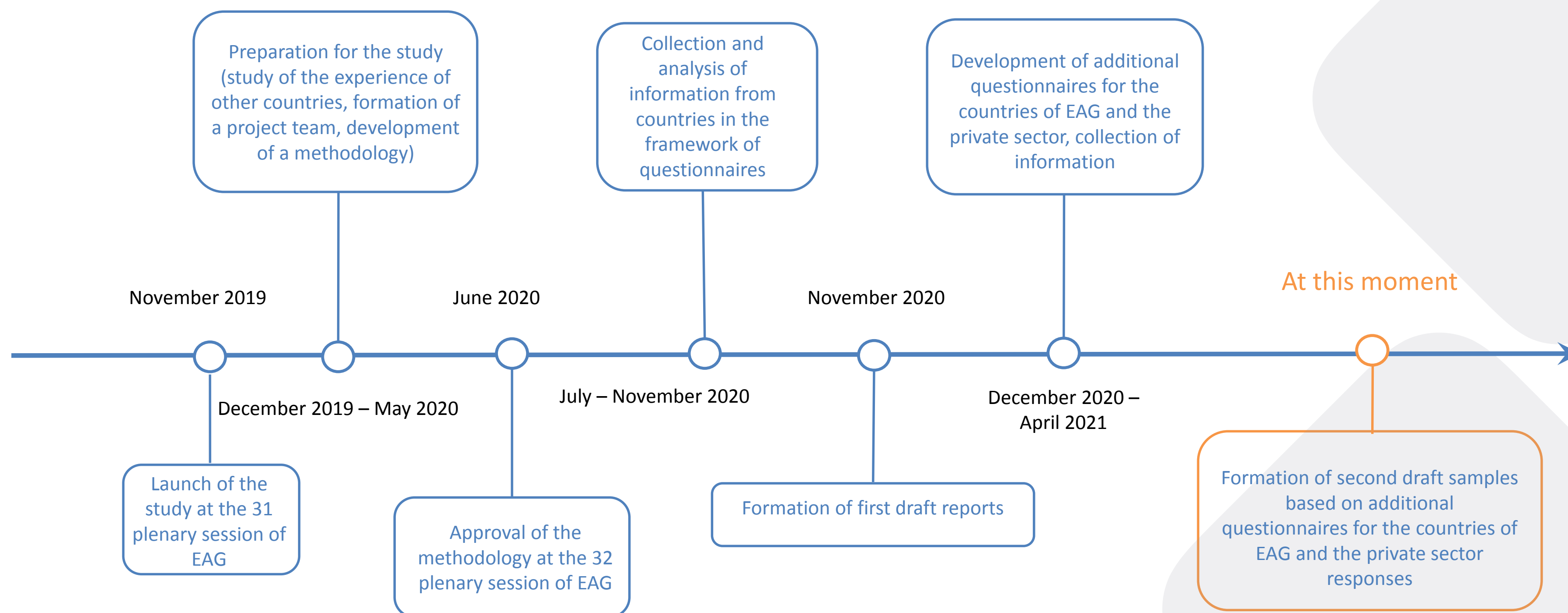
---

***APRIL 28-29, 2021***

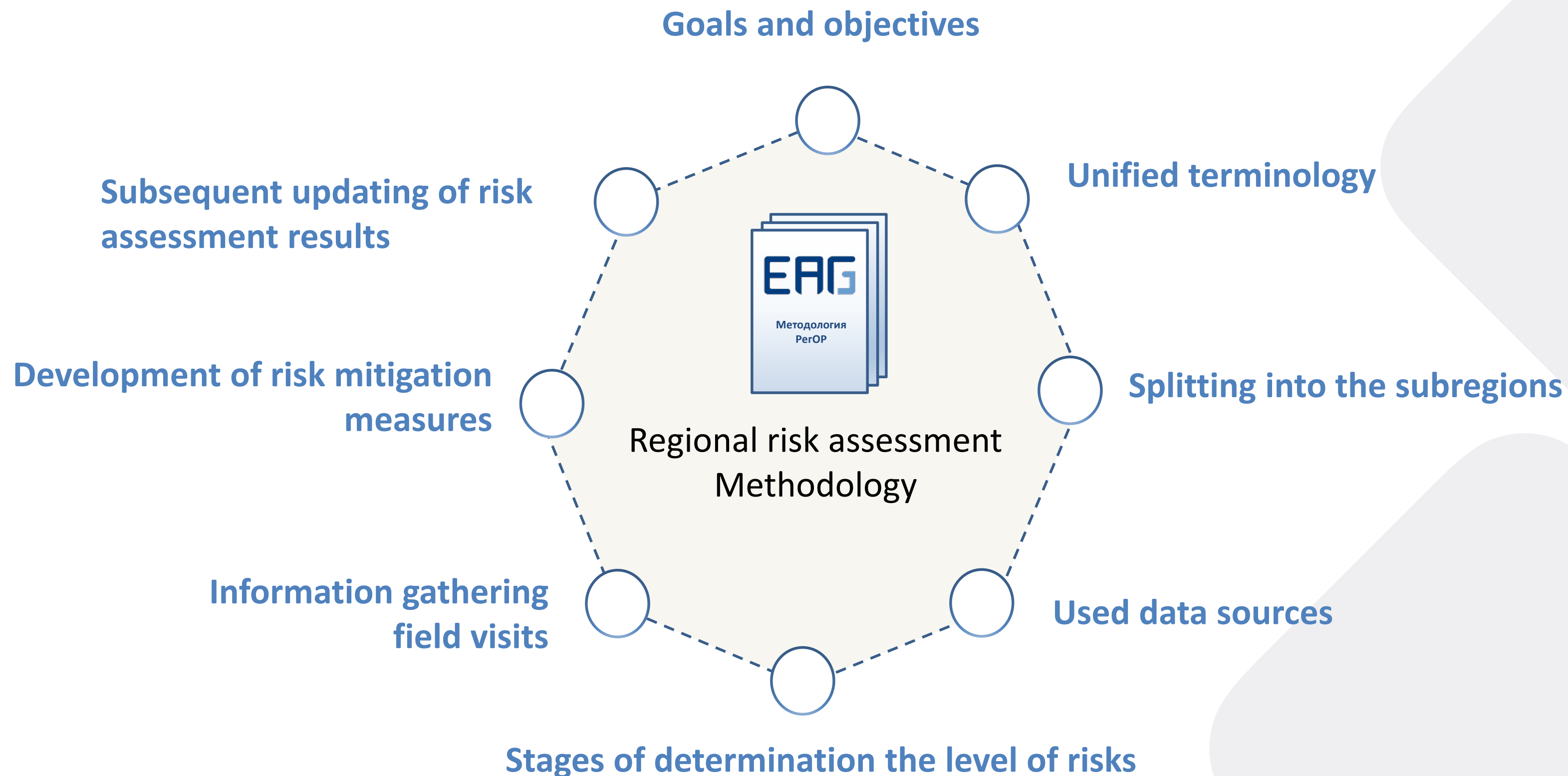


---

# Eurasian region ML/TF Risk Assessment Methodology



# Methodology of regional risk assessment





## Identification of risks



Questionnaire for identifying ML schemes / TF methods

- List of schemes / methods
- Frequency of their use
- Involved countries

## Understanding the risks



Questionnaires for identifying threats and vulnerabilities

- Use of the methods and financial instruments for ML/TF
- Assessment of threats
- Frequency of offences committed by criminal groups
- Assessment of vulnerabilities

# Structure of regional risk assessment reports

Reports  
for each of the four  
regions

- ✓ Key threats in the subregion
- ✓ Key vulnerabilities in the subregion
- ✓ Region-level risks

# Calculation of the risk level of the regional level

1 **Periodicity**  
**Amount of funds**

Summary values for each scheme based on the questionnaires completed by the countries

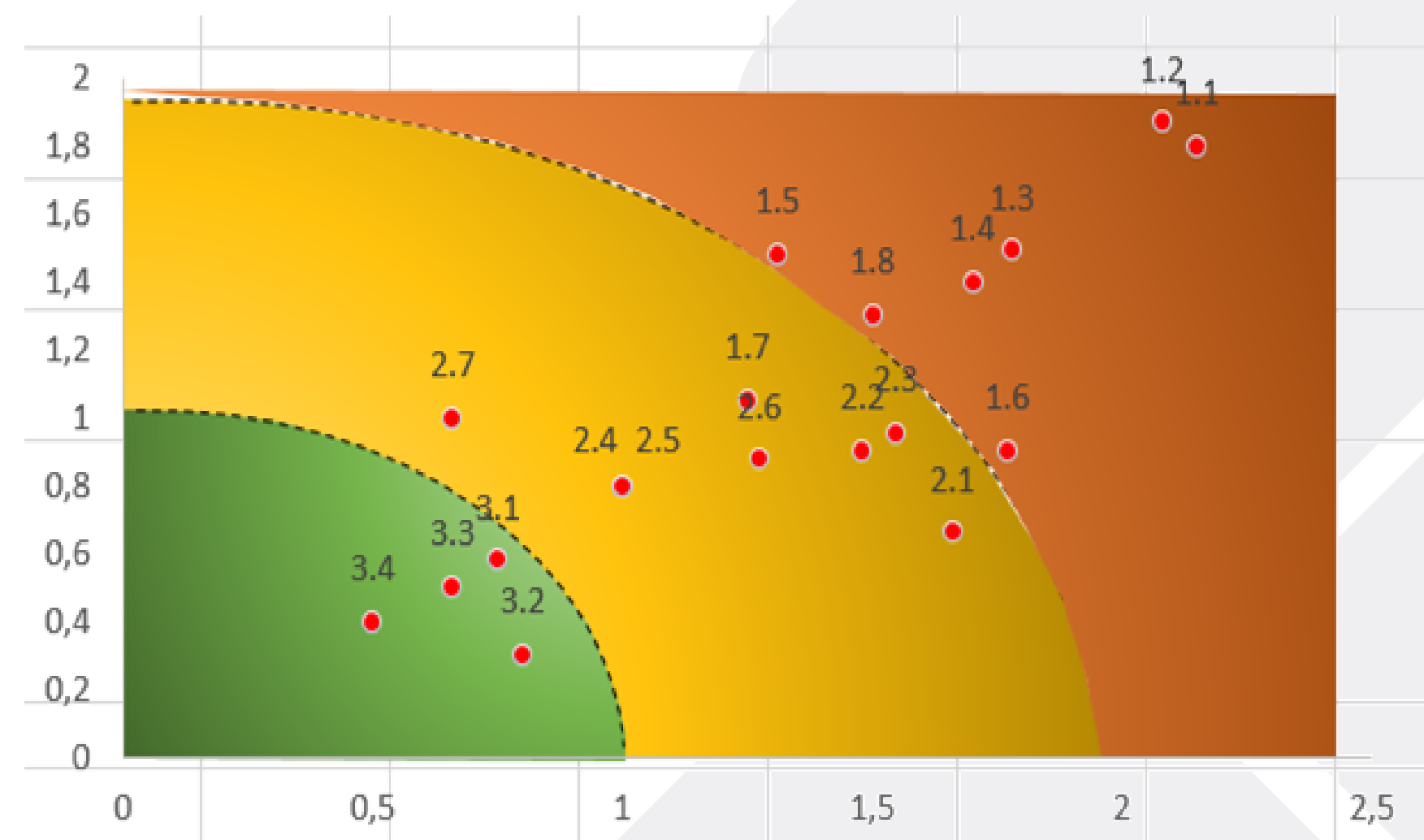
2 **Definition of risk** as a set of schemes, taking into account their manifestation in the commission of various types of crimes. Calculation of the summary values of the frequency and amount of funds for each risk.

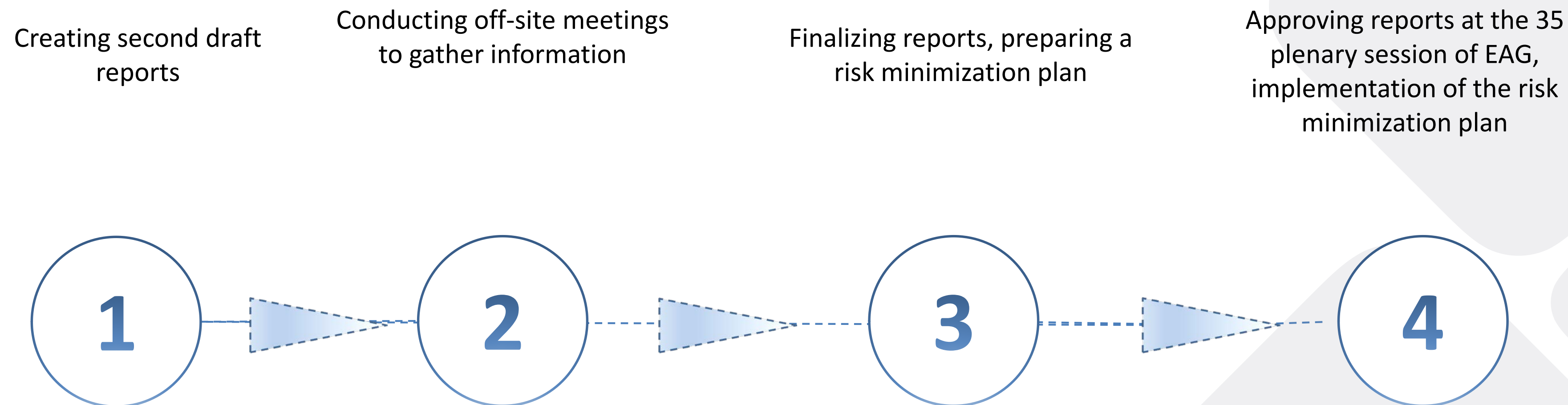
3 Risk = 
$$\sqrt{\text{Periodicity}^2 + \text{Amount of funds}^2}$$

# Calculation of risk ratings and their visualization on the heat map

Regional risks that require significant attention and increased measures to reduce them (from 2 to 3 points inclusive)	
1.1.	Use of fictitious and controlled companies
1.2.	Carrying out transactions related to cash withdrawal, including the purchase of cash proceeds
1.3.	Conducting transit operations on bank accounts
1.4.	Acquisition of movable/immovable property in the territory/outside the state (integration stage)
1.5.	Use of electronic means of payment and cryptocurrencies
1.6.	Investing criminal income in the creation of enterprises or making contributions to the authorized capital of legal entities, including those located in third countries (integration stage)
1.7.	Use of offshore companies
1.8.	Use of fictitious legal entities and individual entrepreneurs
Regional risks that require constant monitoring and enhanced measures to reduce them (from 1 to 2 points inclusive)	
2.1.	Use of trust managers, trusts, lawyers and other persons providing asset management services
2.2.	The transfer of the proceeds of crime outside the subregion and the subsequent return to the countries of the subregion in the form of investments in legitimate commercial activities
2.3.	Legalization of funds stolen through cyber attacks
2.4.	Through the use of charitable foundations
2.5.	Use tour operators
2.6.	Use of non-tangible assets
Regional risks that require taking standard measures to reduce them (from 0 to 1 points inclusive)	
3.1.	Use money transfer systems without opening an account
3.2.	Conducting transactions related to the purchase of goods, content and services on the Internet
3.3.	Withdrawal of funds abroad using enforcement instruments
3.4.	Use cash couriers
3.5.	Use of bank securities for the purpose of converting money into foreign currency, withdrawing it and cashing it out

The heat map





**Thank you for attention!**

Ak Bars  
Bank



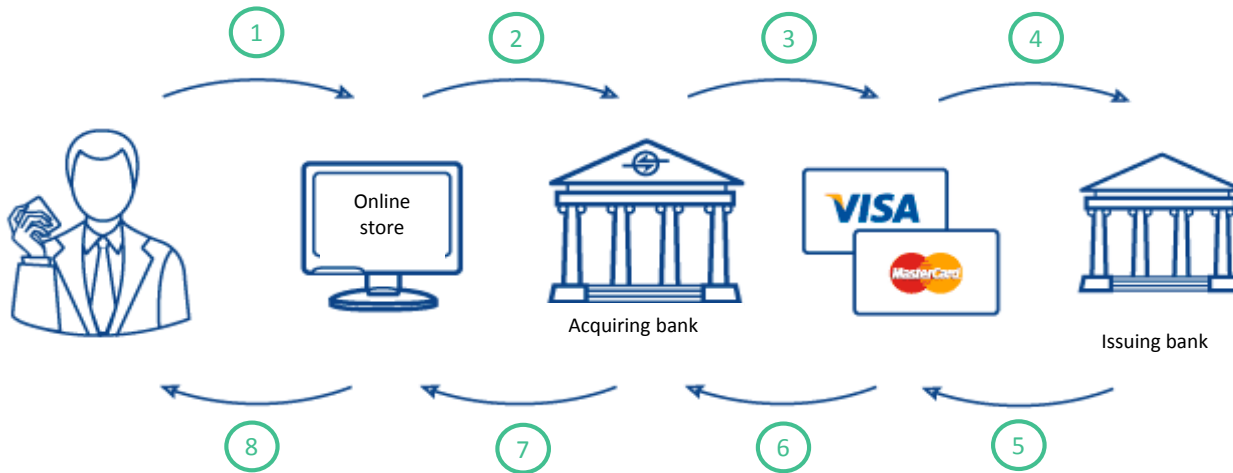
# **AML risks in Internet acquiring. The ways of their minimizing.**





# What is it all about?

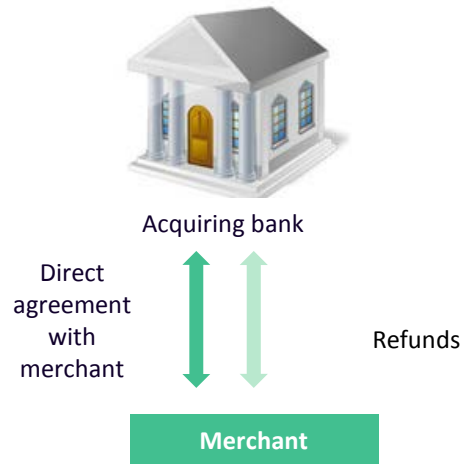
**Internet acquiring is a general term for accepting plastic and virtual cards payments via the Internet using a specially developed web interface.**



1. The customer makes a purchase in an online store.
2. After authentication, the Provider sends the information for the authorization request to the acquiring Bank.
3. The acquirer sends a request for authorization of the transaction to the international payment system.
4. IPS generates a request to the issuing Bank
5. The issuing Bank generates a response to the IPS request
6. The IPS transmits the response to the acquiring Bank.
7. The acquiring Bank transfers the reimbursement for completed transactions to the account of the online store and transmits information about the payment status to the online store.
8. The user receives the order results.

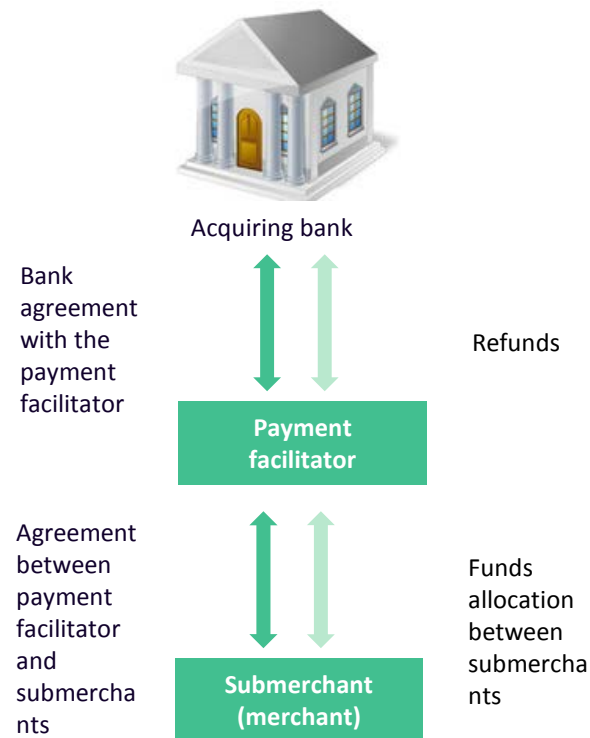
# Patterns of communication with online stores

## Direct agreement conclusion between the Bank and the merchant



- Direct conclusion of an agreement between the Bank and the merchant
- Merchant verification and identification
- Possibility to attract a provider to render additional services when accepting payments (personal account, reports, etc.)

## With the involvement of a payment facilitator



- The Bank does not enter into an agreement with the merchant.
- The distribution of funds between the merchant is carried out by the payment facilitator.
- The Bank interacts only with the payment facilitator.

# Types of risks in Internet acquiring

Risks in Internet acquiring are primarily associated with the quality of merchants being serviced

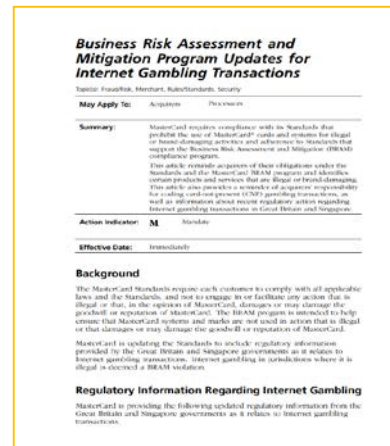
## Financial risks:

- losses on disputed transactions (chargebacks);
- commissions and fines from international payment systems (IPS) for exceeding the fraud level, prohibited activities, violation of the work rules;
- fines of the Bank of Russia for non-compliance with legal requirements.

## Legal and reputational risks:

- loss of business reputation by the bank;
- termination of cooperation with clients and partners;
- consequences from lawsuits by cardholders.

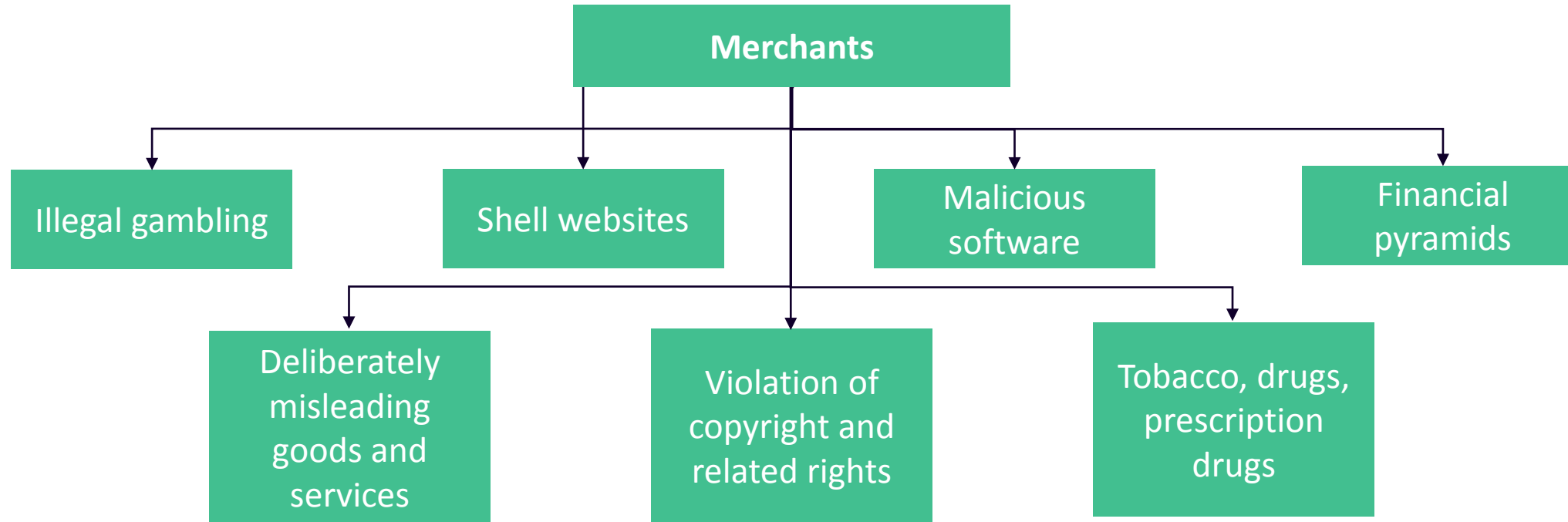
*\* there are known cases of cardholders specifically looking for violations of current legislation in the banks' activities (particularly frequent in AML and combating the terrorist financing), filing complaints to the Central Bank, Federal Service for Financial Monitoring and law enforcement authorities.*



The risks associated with acquiring are described in detail in the IPS documentation:

The rules and measures to protect Visa brand are described in the Global Brand Protection Program (GBPP), a similar MasterCard program is called the Business Risk Assessment and Mitigation (BRAM).

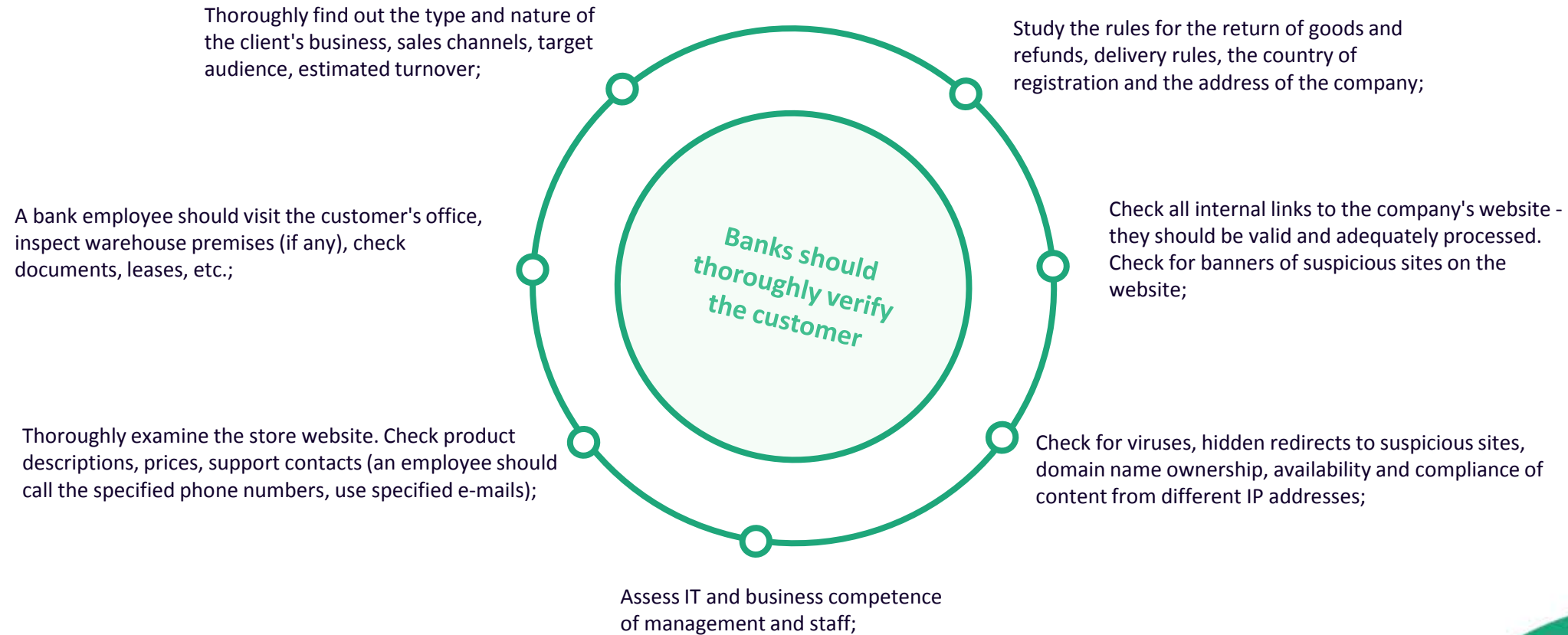
# Types of risks in Internet acquiring



In order to engage in Internet acquiring avoiding sanctions and fines, banks are to carefully monitor their acquiring clients. When working through facilitators, this becomes much more difficult, since in many ways the level of risk depends on the partner trustworthiness

# What does AML have to do with it?

To mitigate risks in Internet acquiring, banks are obliged to possess certain maturity level in implementation of Know Your Customer (KYC) principle.



# Patterns using miscoding

**Miscoding is a separate type of fraud in a bank acquiring network involving spoofing the purpose of payment.**

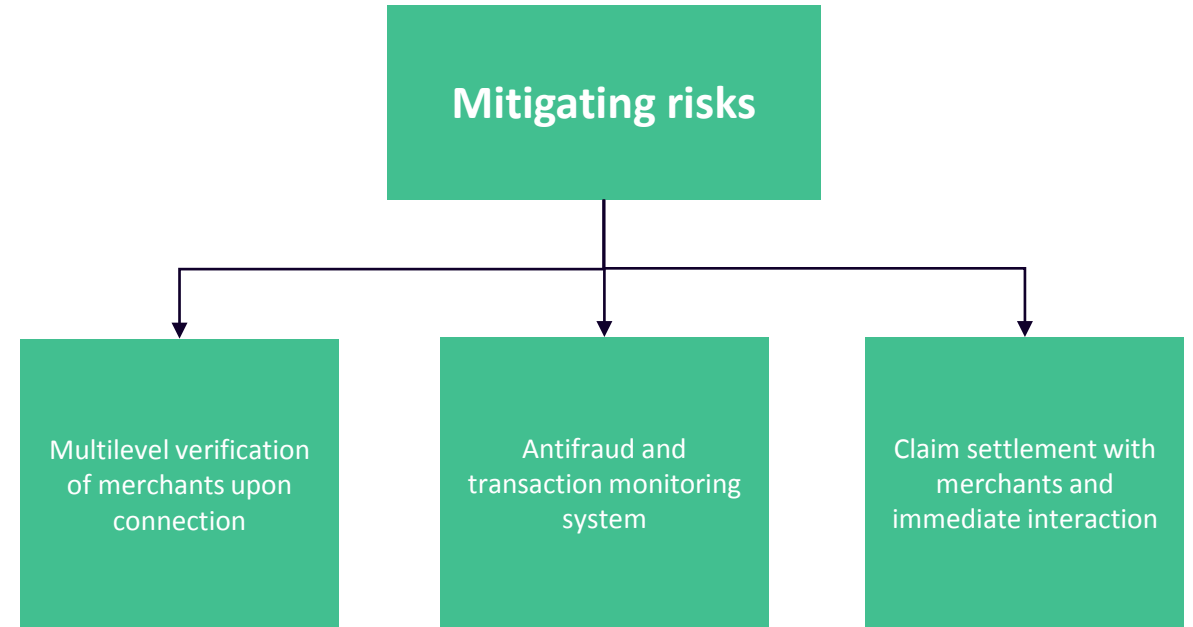
- Most often, miscoding being used by illegal online casinos and bookmakers. As regards illegal gambling business, amid a legislative ban on its activities, it is vitally necessary to ensure the acceptance of bets from bank cards and replenishment of gaming accounts.
- Also, such a pattern is used by crypto exchangers and online scammers to directly deceive consumers.
- Those companies with the appropriate permissions to conduct gambling activities are the only ones to legally obtain an acquiring terminal with the merchant code MCC 7995 Betting/Casino Gambling. This is usually strictly regulated and verified by Visa and MasterCard payment systems and the acquiring bank.
- Due to miscoding, unscrupulous market participants manage to fraudulently pass the initial audit of the financial monitoring of the Bank with the terminal registered. With this objective, they declare any other activity - accepting payments for housing and communal services, training, online cinemas, trade and services, etc., and the website changes its content. This undisclosed pattern can be considered a classic example of money laundering.
- The acquiring Bank should identify all transactions of this kind, and the card issuing Bank is to identify the nature of these transactions. The substitution and use of fake MCC codes is a gross violation of the IPS rules.

МСС код: 0000, 0763, 1799, 2791, 2842, 4214, 4225, 4813, 4815, 4829, 4900, 5044, 5046, 5047, 5051, 5169, 5199, 5271, 5551, 5935, 5960, 5962, 6010, 6011, 6012, 6022, 6023, 6025, 6026, 6028, 6050, 6051, 6211, 6381, 6399, 6513, 6529, 6530, 6531, 6532, 6533, 6534, 6535, 6536, 6537, 6538, 6540, 6611, 6760, 7012, 7273, 7276, 7277, 7279, 7280, 7311, 7321, 7322, 7372, 7389, 7392, 7393, 7511, 7995, 8111, 8211, 8220, 8241, 8244, 8249, 8299, 8398, 8641, 8651, 8661, 8675, 8699, 8734, 8911, 8931, 9211, 9222, 9223, 9311, 9399, 9401, 9402, 9405, 9411, 9702, 9753, 9950

# Ways to strengthen internal control in Internet acquiring

Banks often have **internal control deficiencies** at the following stages:

- customer capture, preliminary screening of high-risk merchants;
- checking online stores, analyzing client activities and information update;
- online store profiling (average turnover, average check, etc.) and tracking changes in behavior and customer profile;
- registration of terminals and assignment of MCC code (miscoding risk);
- control over the use of terminals, the specification of key risk indicators;
- fraud monitoring and responding;
- the control mechanisms of banks in Internet acquiring are not described in their internal rules.



Law enforcement authorities in some countries use sample purchases as one of the mechanisms for detecting violations in Internet acquiring. Similar tools could significantly improve the efficiency of the credit institution's internal control system.



Ak Bars  
Bank



**Thank you  
for your  
attention.**

**Akbars.ru**

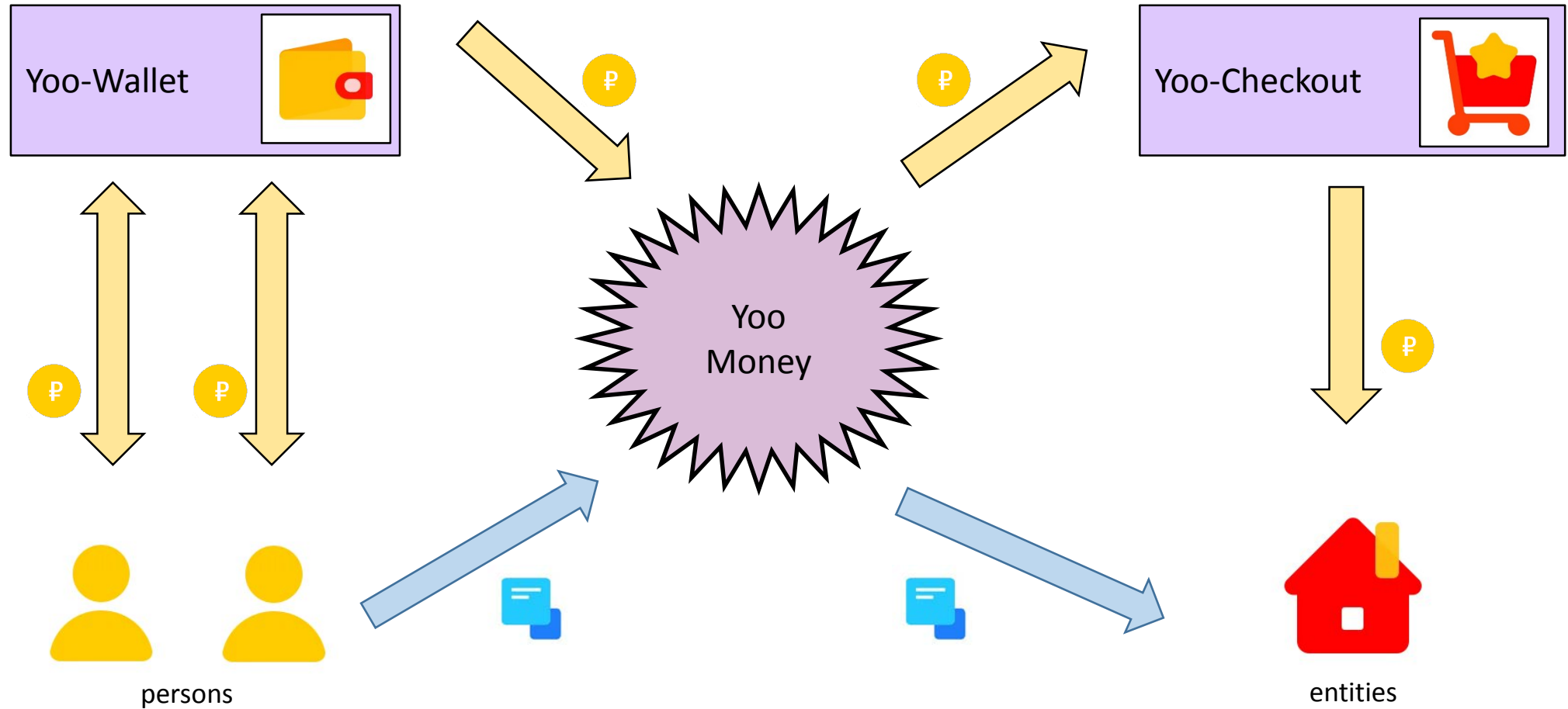




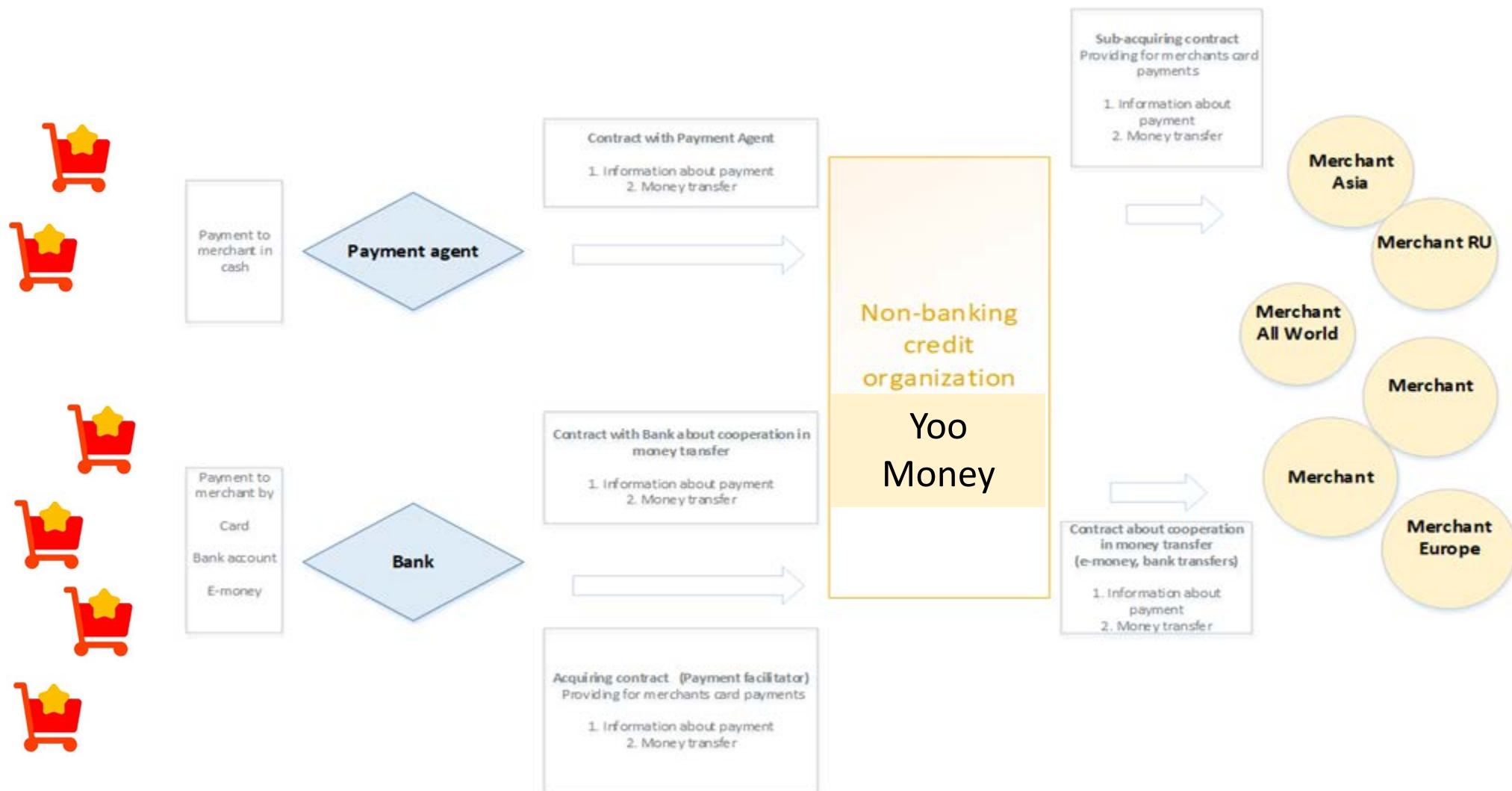
# Illegal typologies in E-wallet service and automated measures for its detection

**Dmitriy Gronin,**  
Head of Compliance Department

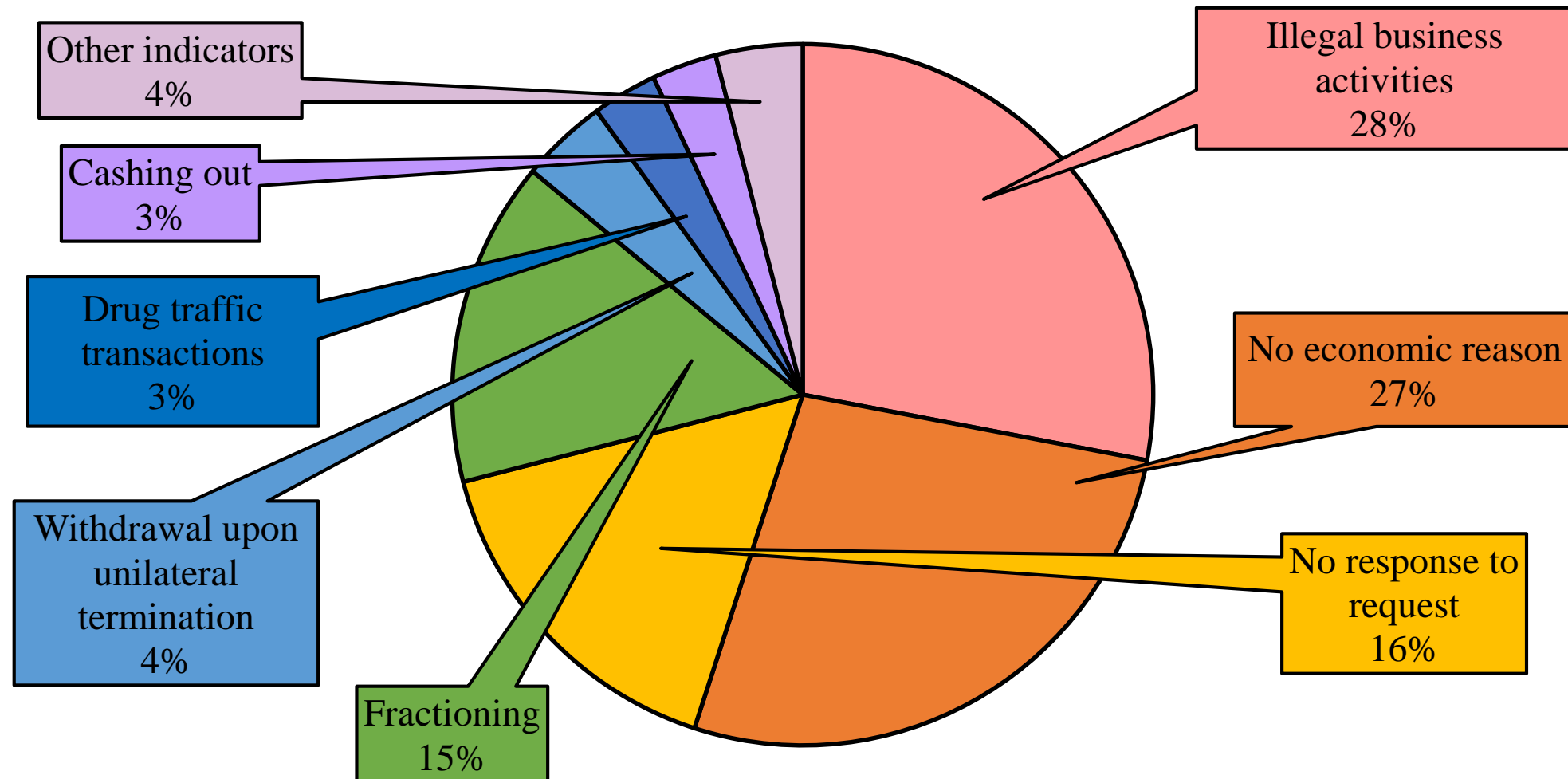
# Our basic services



# Yoo-Checkout



# Structure of the main reporting areas in 2020



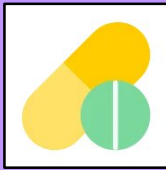
# Illegal typologies

## Illegal business activities



- Products and services providing;
- Paid content sharing;
- Criptoexchange;
- Currency exchangers;
- Money transfer systems;
- Collecting investments/pyramids.

## Forbidden products turnover



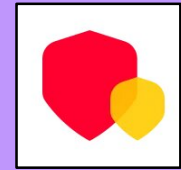
- Narcotic drugs;
- weapon;
- Chemical active stuff and explosives;
- Turnover of virtual values (counterfeit).

## Cashing out by «drops»



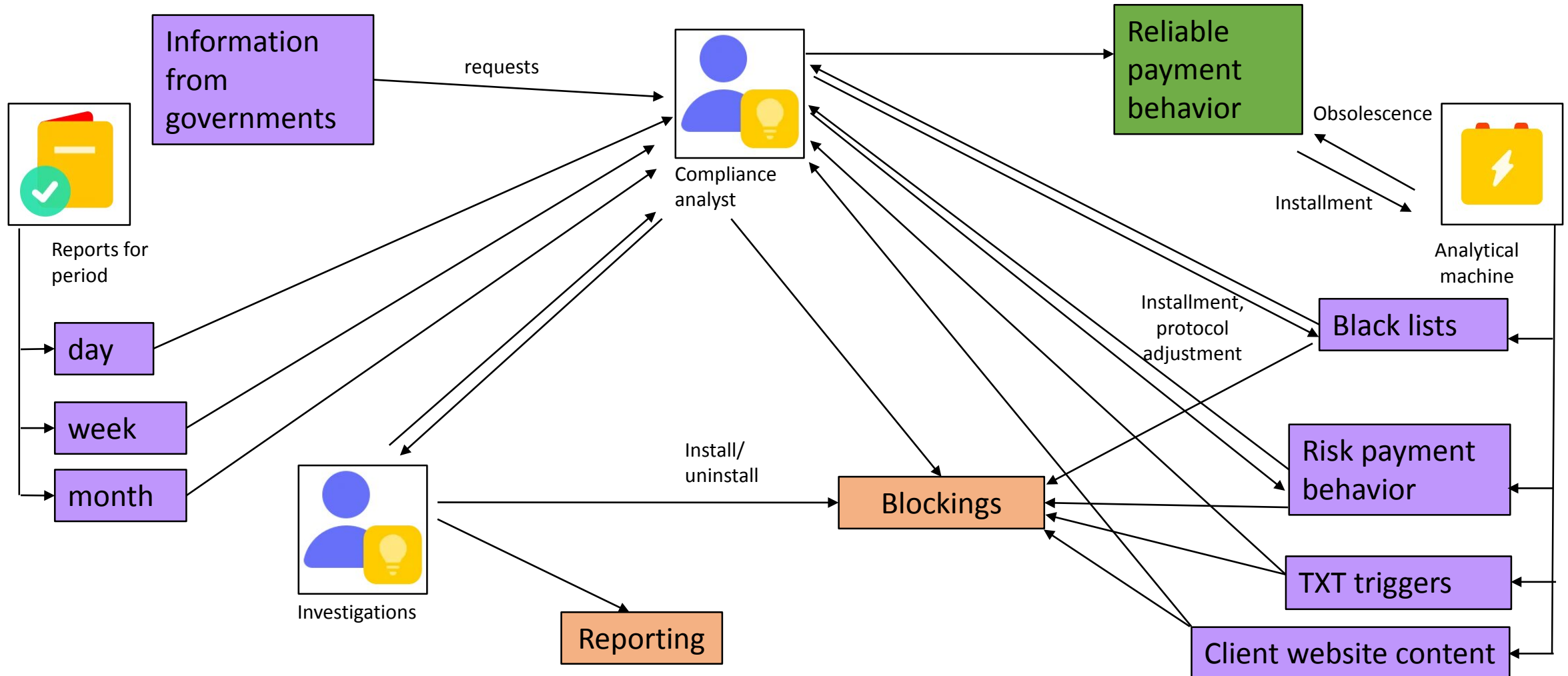
- Tax evasion;
- Budget violations;
- Formation of the bribery mass;
- Misappropriation;
- Fake bills stuffing;
- Fraud.

## Account takeover and other



- Account hacking technically;
- Social engineering;
- Forgery of notarial and other documents;
- "Scheme" with fictitious executive documents.

# Monitoring the flow of electronic money







## Global overlap

devices, cookies

digital identities

payment tools

geo-location

emails

phones

IPs

...



## Artificial intelligence (analytical machine)

- Self-training online robot for merchant's sites check;
- Anti-account takeover models;
- Payment anomaly detection;
- Merchant fraudulent and anomaly detection models (including price and feedback monitoring);
- Identifying robotic wallet management

---

# Regional methods of money laundering. Presentation of the results of the preliminary survey of the private sector

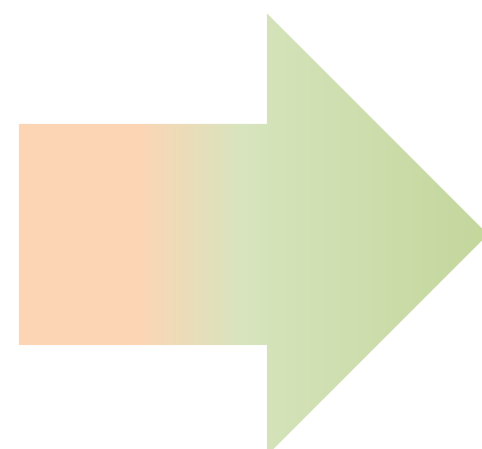
## 1 From the accounts of being shell companies

Method ML	Average value	Countries						
		Kazakhstan	Kyrgyzstan	Tajikistan	Uzbekistan	Russia	China	Turkmenistan
domestically								
with further transfer to accounts held by legal entities suspected of being shell companies;	1,57	1,28	1,37	1,30	2,50	3,00	2,00	0,00
with further transfer to accounts held by individual entrepreneurs;	1,42	1,42	1,00	1,20	1,50	2,60	2,00	0,00
with further transfer to accounts held by natural person;	1,40	1,35	0,75	1,20	1,50	3,00	2,00	0,00
with further transfer to offshore jurisdictions								
to accounts held by foreign legal entities suspected of being shell companies;	1,35	1,35	1,25	1,20	1,50	2,20	1,00	0,00
to accounts held by foreign legal arrangements;	1,14	1,50	1,25	0,90	0,50	1,40	0,00	0,00
with further transfer to the Eurasian Region countries								
to accounts held by foreign legal entities suspected of being shell companies;	1,19	1,07	1,00	1,40	1,00	1,80	1,00	0,00
to accounts held by foreign legal arrangements;	1,00	1,00	1,25	1,10	0,50	1,20	0,00	0,00
with further transfer to other countries								
to accounts held by foreign legal entities suspected of being shell companies;	1,23	1,14	1,25	1,20	1,00	2,00	1,00	0,00
to accounts held by foreign legal arrangements.	1,07	1,35	1,25	0,90	0,50	1,20	0,00	0,00

ML risk from the interim subregion report:  
«Using shell and/or controlled companies»

# Trends of using legal persons in ML schemes

Classic  
nominee  
companies



Real  
companies

# Misuse/participation of the different types of persons

Type	Average value	Countries						
		Kazakhstan	Kyrgyzstan	Tajikistan	Uzbekistan	Russia	China	Turkmenistan
Limited liability companies (partnerships)	1,75	1,85	1,66	1,33	2,50	2,75	1,50	0,00
Natural persons	1,70	1,85	1,44	1,55	2,00	2,75	1,00	0,00
Individual entrepreneurs	1,61	1,78	1,30	1,55	1,50	2,00	2,00	1,00
Funds	1,25	1,28	1,12	1,44	1,00	1,75	0,50	0,00
Joint-stock companies	1,04	0,78	1,11	1,33	2,00	0,75	1,50	0,00
Legal arrangements	0,97	1,08	1,42	0,87	0,50	1,00	0,00	0,00
Consumer cooperatives	0,92	1,30	0,44	1,11	0,50	1,25	0,00	0,00

## ② Using bank accounts and cards held by natural persons

Method ML	Average value	Countries						
		Kazakhstan	Kyrgyzstan	Tajikistan	Uzbekistan	Russia	China	Turkmenistan
Bank accounts and cards held by natural persons	1,47	1,21	1,25	1,30	1,00	2,80	3,00	0,00

ML risk from the interim subregion report  
«Money laundering with the use of bank accounts and cards»



# Movement of funds with the use of unregulated entities

Method ML	Average value	Countries						
		Kazakhstan	Kyrgyzstan	Tajikistan	Uzbekistan	Russia	China	Turkmenistan
Virtual currency service providers;	0,85	0,78	0,37	1,20	0,50	1,80	0,00	0,00
Operators of informal money or value transfer systems (hawala, etc.).	0,76	0,35	0,50	0,80	1,00	1,60	2,00	1,00
Operators of payment systems that enable to transfer title units among users allowing them to pay for goods and services;	0,64	0,57	0,25	0,90	1,00	1,20	0,00	0,00

ML risk from the interim subregion report «Using electronic payment instruments and cryptocurrencies», «Using money mules»



# Conversion of non-cash funds into cash

Method ML	Average value	Countries						
		Kazakhstan	Kyrgyzstan	Tajikistan	Uzbekistan	Russia	China	Turkmenistan
Withdrawal from of cash from cards held by natural persons	1,78	1,71	2,00	1,40	1,50	2,80	2,00	0,00
Withdrawal of cash from corporate bank cards of legal entities that are suspected of being shell companies	1,33	1,64	0,50	1,20	1,00	3,00	0,00	0,00
Purchase of foreign currency cash	1,52	1,50	1,62	1,60	1,00	2,00	1,00	0,00

ML risk from the interim subregion report «Conducting cash-out operations, including purchase of cash receipts»

# Conversion of cash into non-cash funds

Method ML	Average value	Countries						
		Kazakhstan	Kyrgyzstan	Tajikistan	Uzbekistan	Russia	China	Turkmenistan
by depositing cash into accounts held by natural persons;	1,69	1,64	2,25	1,20	1,50	2,20	2,00	0,00
by depositing cash into accounts of entities involved in real financial and business activities;	1,23	1,14	2,12	1,10	0,50	0,80	1,00	1,00
through cash offices of entities suspected of being shell companies;	1,00	0,85	0,75	1,10	1,50	2,00	0,00	0,00
by purchasing bills for cash	0,47	0,07	0,5	0,50	0	2,00	0,00	0,00

ML risks from the interim subregion report:

- ❑ «Using sham legal entities and individual entrepreneurs»,
- ❑ «Money laundering with the use of bank accounts and cards»

# Movement of cash

Method ML	Average value	Countries						
		Kazakhstan	Kyrgyzstan	Tajikistan	Uzbekistan	Russia	China	Turkmenistan
Sale and purchase of foreign currency cash	1,75	1,71	2,75	1,80	1,50	0,75	1,00	0,00
<i>money transfers without opening bank accounts</i>								
to/from natural persons located in other countries;	1,57	1,21	2,50	1,30	1,50	1,60	2,00	1,00
to/from natural persons located in your country;	1,54	1,07	2,25	1,70	1,50	2,00	1,00	0,00
to/from natural persons located in countries featured by enhanced illicit drug trafficking operations	1,30	1,00	1,00	1,60	2,00	1,80	2,00	0,00

ML risk from the interim subregion report  
 «Using money transfer systems without opening an account»,  
 «Using money mules»

## ① Depositing funds into bank/ deposit accounts

Method ML	Average value	Countries						
		Kazakhstan	Kyrgyzstan	Tajikistan	Uzbekistan	Russia	China	Turkmenistan
Depositing funds into bank/ deposit accounts	1,69	1,42	2,37	1,50	1,00	2,00	2,00	1,00

ML risk from the interim subregion report «Money laundering with the use of bank accounts and cards»

## ② Transactions with immovable (real estate) property

Method ML	Average value	Countries						
		Kazakhstan	Kyrgyzstan	Tajikistan	Uzbekistan	Russia	China	Turkmenistan
with cash payment								
domestically;	1,48	1,57	2,14	1,10	2,00	1,40	0,00	2,00
in the Eurasian Region countries;	0,89	0,85	1,20	1,22	0,50	0,80	0,00	0,00
in offshore jurisdictions;	0,89	1,00	0,60	1,33	0,50	0,80	0,00	0,00
in other courtiers.	0,76	0,71	0,60	1,33	0,50	0,60	0,00	0,00
with non-cash payment								
domestically;	1,30	1,50	1,75	0,70	0,50	1,4	2,00	1,00
in the Eurasian Region countries;	1,00	0,92	1,71	0,80	0,50	1,00	1,00	0,00
in other courtiers;	0,97	0,78	1,42	1,00	1,00	1,00	1,00	0,00
in offshore jurisdictions.	0,92	1,07	0,57	1,10	0,50	1,00	1,00	0,00

ML risk from the interim subregion report «Acquisition of movable/ immovable property in the country /abroad»

### 3 Other methods

Method ML	Average value	Countries						
		Kazakhstan	Kyrgyzstan	Tajikistan	Uzbekistan	Russia	China	Turkmenistan
Repayment of early received loans;	1,20	1,14	1,57	1,33	0,00	1,40	1,00	0,00
Payment for legal services;	1,02	1,21	1,37	0,80	0,00	1,40	0,00	0,00
Purchase of precious metals, precious stones and jewelry;	1,02	0,71	1,12	1,10	1,00	1,40	1,00	2,00
Payment for notary services;	0,83	1,00	1,37	0,40	0,00	1,20	0,00	0,00
Transfer of funds into trust management to foreign legal arrangements;	0,80	0,64	0,71	0,90	0,00	1,60	1,00	0,00
Payment for audit services;	0,75	0,85	1,00	0,60	0,00	1,20	0,00	0,00
Purchase of bills.	0,65	0,21	1,14	0,70	0,00	1,80	0,00	0,00

ML risk from the interim subregion report «Using trustees, trusts, lawyers and other persons providing asset management services»

**Thank you for attention!**

Topic: Entities Subject to Increased  
Monitoring.

The Profile of a High-risk Client  
and His/Her Financial Behavior (customers -  
legal entities).

“UZPROMSTROYBANK” Joint-Stock Commercial Bank



# Introduction: Relevance of the Topic

- FATF Standards and national legislation of Uzbekistan;
- AML/CFT/CPF system of Uzbekistan;
- 2008 crisis, COVID-19 pandemic;
- Technological and current aspects of ML/TF/PF risks

# Role of Regulators in Improvement of CDD Mechanisms: Methodology

- Practices of banks and other entities + updating;
- Forwarding of recommendations to banks;
- New technologies information hub;
- Statistical information on fraud incidents encountered by banks;
- Co-developer of AML/CFT/CPF regulations and guidelines

# Role of Regulators in Improvement of CDD Mechanisms: Practical Cases

- Transactions are consistent with business activities, analysis of operating locations raises doubts;
- Sudden large turnover;
- Secondary and subsequent accounts;
- Operating locations and places of customer registration do not match;
- Large turnover of customer corporate cards;
- Loans are the sources of income of a legal entity;
- Large cash inflows (export revenues, contributions to the authorized capital).

# Role of FIU in Improvement of CDD Mechanisms: Methodology

- Although the FIU is primarily focused on economic and financial crimes, it also deals with other criminal offences;
- Source of information on international foreign exchange transaction schemes;
- The only source of information on cross-border cash transportation;
- The widest access to international and domestic databases containing information on natural/legal persons;
- Suspicious transactions carried out by all entities are accumulated in the FIU;
- Hub accumulating practical schemes and methods of illegal transactions, including those related to ML/TF;
- The FIU has a set of training manuals and methodological guidelines covering the profiles of high-risk legal entities, including criminal groups.

# Role of FIU in Improvement of CDD Mechanisms: Practical Cases

## *Case A: Types of activities that are subject to licensing:*

- One or more incoming transactions of a customer are subject to mandatory licensing based on the payment details and contract purposes, but the customer has no license to carry out such activity;
- One or more incoming transactions of a customer are subject to mandatory licensing based on the payment details and contract purposes, but the license held by the customer is granted for carrying out other type of activity;
- Measures recommended by the FIU:
- Monitoring of transactions carried out by legal entities, examination and verification of their licenses.

# Role of FIU in Improvement of CDD Mechanisms: Practical Cases

*Case B: Transactions related to importation of goods or services with involvement of different countries:*

- A resident of the Republic of Uzbekistan imports the goods;
- The value of the imported goods is high, at least several hundred thousand USD;
- The customer contract is registered in the Unified Electronic Information System for Foreign Trade Operations (government register);
- However, the contract indicates that the Manufacturer is located in Country A, the goods will be supplied by the company located in Country B, the counterparty's bank is located in Country C, and the shipper is located in Country D.
- Measures recommended by the FIU:
- Monitoring of transactions carried out by legal entities and reporting of dubious (suspicious) transactions.

# Role of FIU in Improvement of CDD Mechanisms: Practical Cases

*Case C. Transactions involving guarantees of large legal entities:*

- Company A and Company B enter into the loan agreement;
- Company A is the loan recipient and, as a guarantee for Company B, provides loan guarantees to the larger company C (which may be partly owned by the government);
- Since all three companies act in conspiracy, Company A does not repay the loan to Company B, and Company B files a lawsuit in order to recover the funds from Company A;
- Based on the loan guarantee agreement, the court orders Company C to repay the loan to Company B, and Company B quickly transfers the received funds to different legal or natural persons. This scheme allows the conspirators to fraudulently receive funds at the expense of Company C which suffers losses.
- Measures recommended by the FIU:
- Monitoring of transactions carried out by legal entities and enhanced attention to transactions involving guarantee or claim assignment agreements.

# Regional Money Laundering Threats and Vulnerabilities

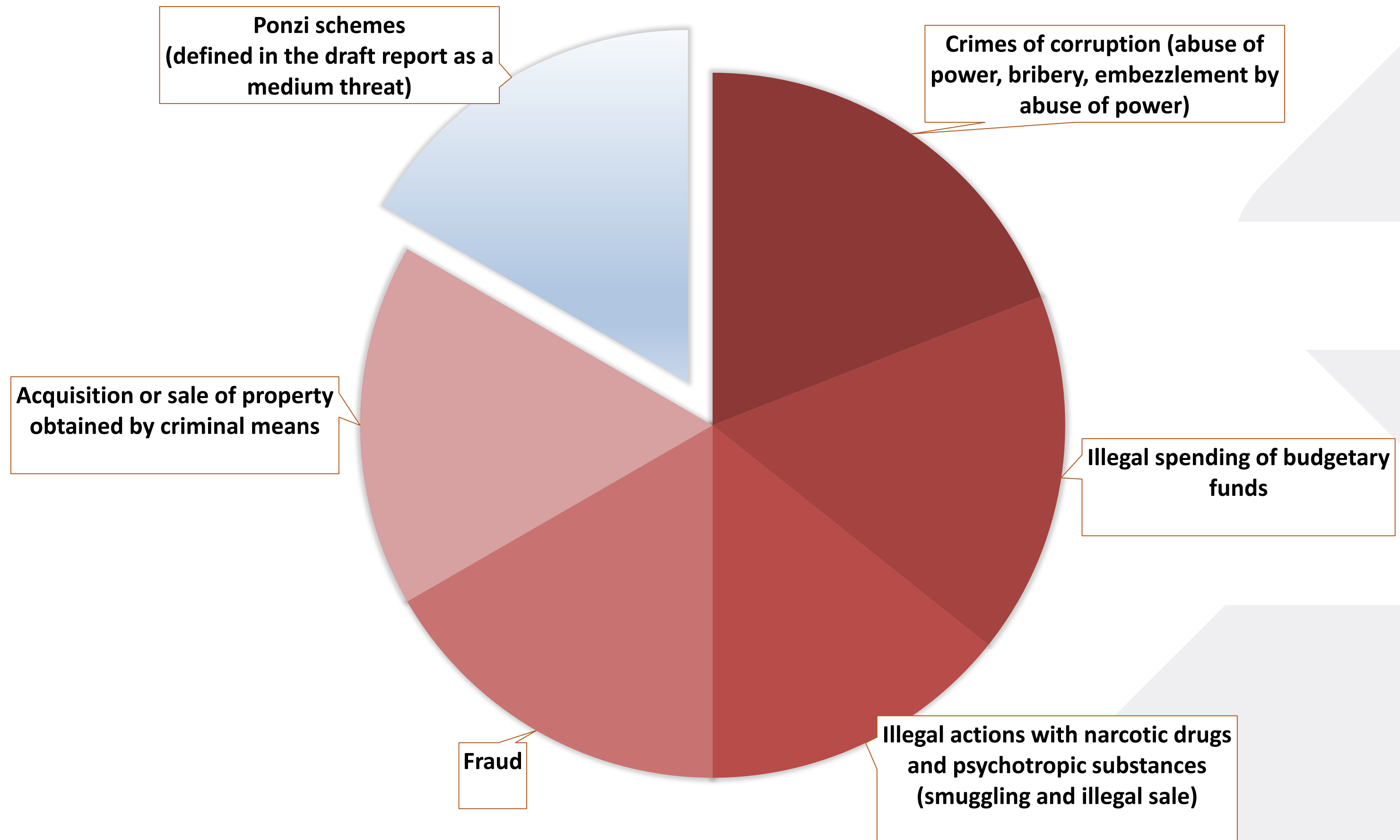
---

The Eurasian Group on Combating Money Laundering and Financing of Terrorism (EAG)

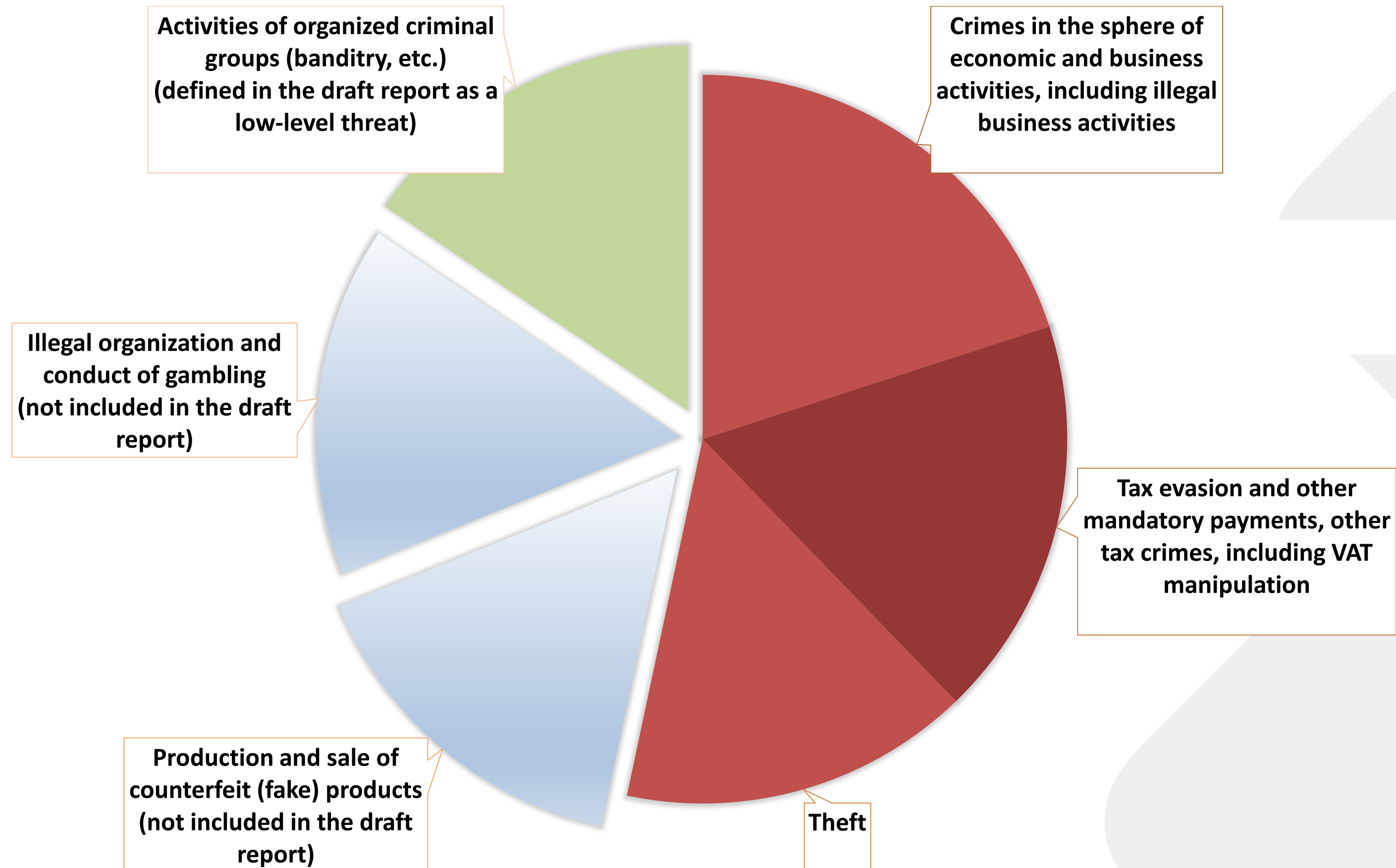
*Speaker: Nazerke Zhampeiis (EAG Secretariat)*



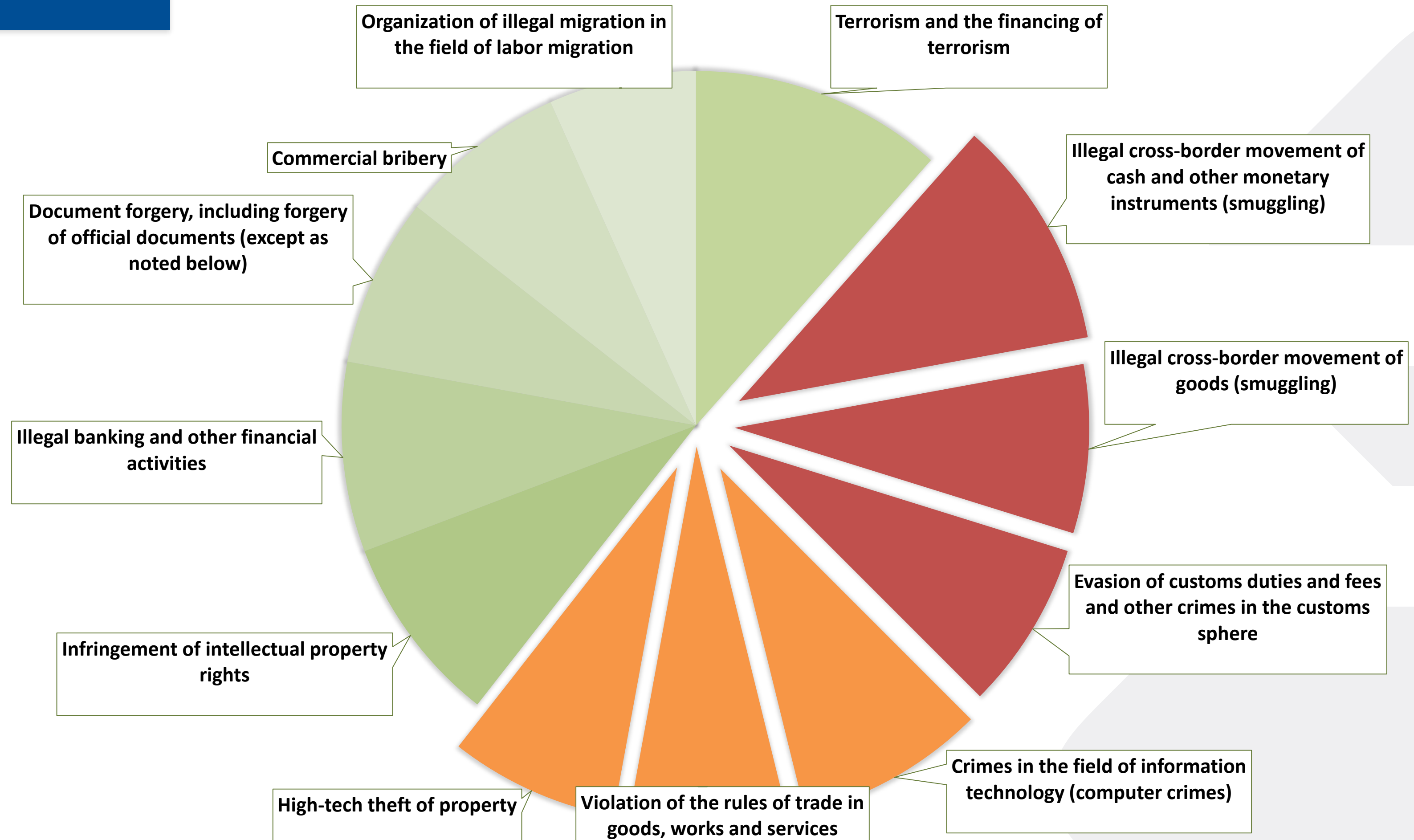
# Threats. High-level sources of criminal income

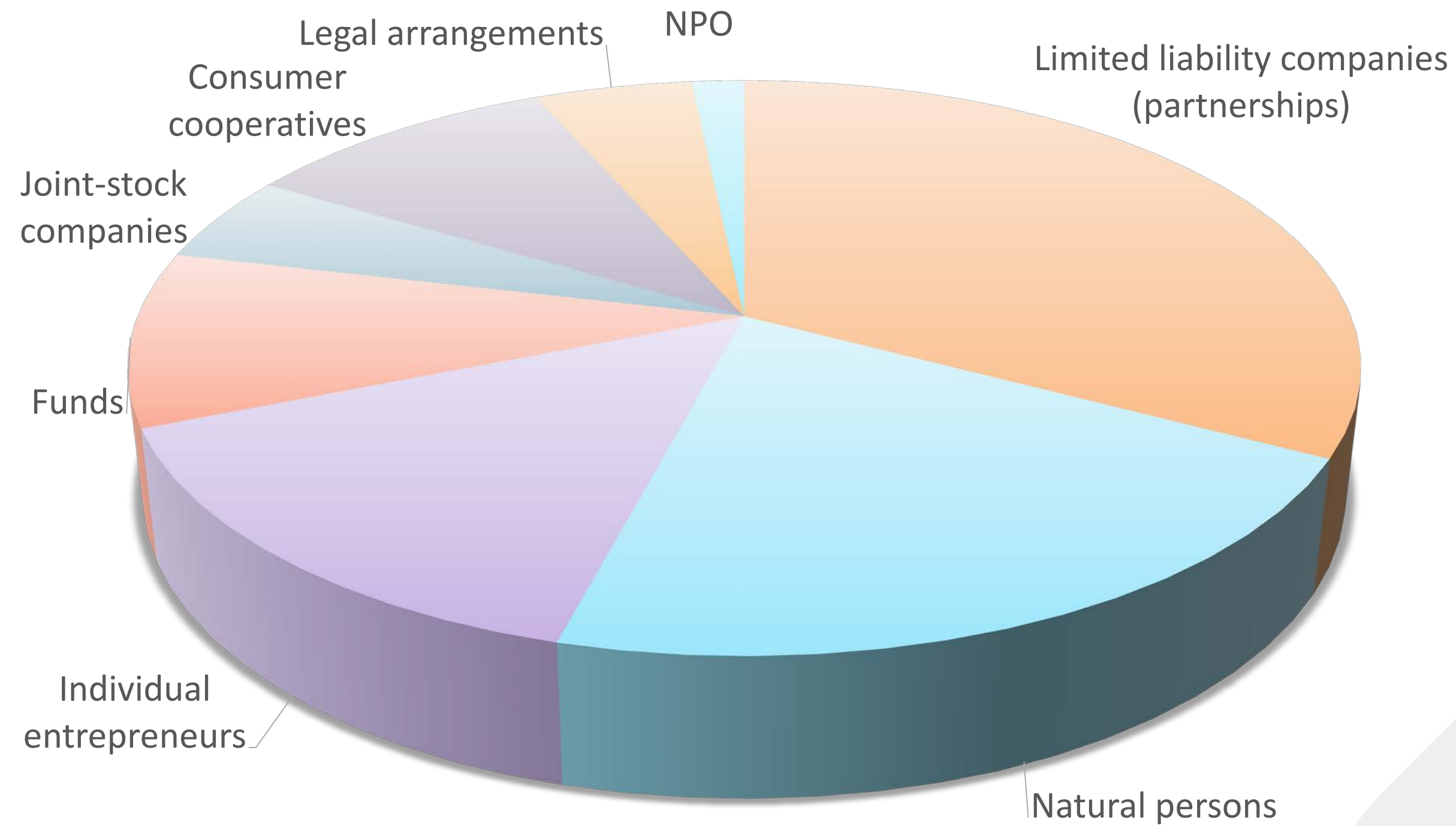


# Threats. Moderate-level sources of criminal income



# Threats. Low-level sources of criminal income





# Vulnerabilities - sectors

## FINANCIAL SECTOR

*(banks and non-bank financial institutions)*



VS

## DNFBPs SECTOR

*(accountants, casinos, dealers in precious metals and stones, organizers of gambling, lawyers, notaries, realtors)*



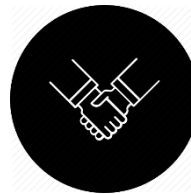
# Vulnerabilities - risk context



**Interest in illegally transferring funds abroad**



**High level of cash payments**



**Gaps in the regulation and implementation of state control**

- with regard to new financial products and services, including electronic money (e-wallets, cryptocurrencies)
- with regard to the shadow sector of the economy



**Ability to use nominal legal entities**



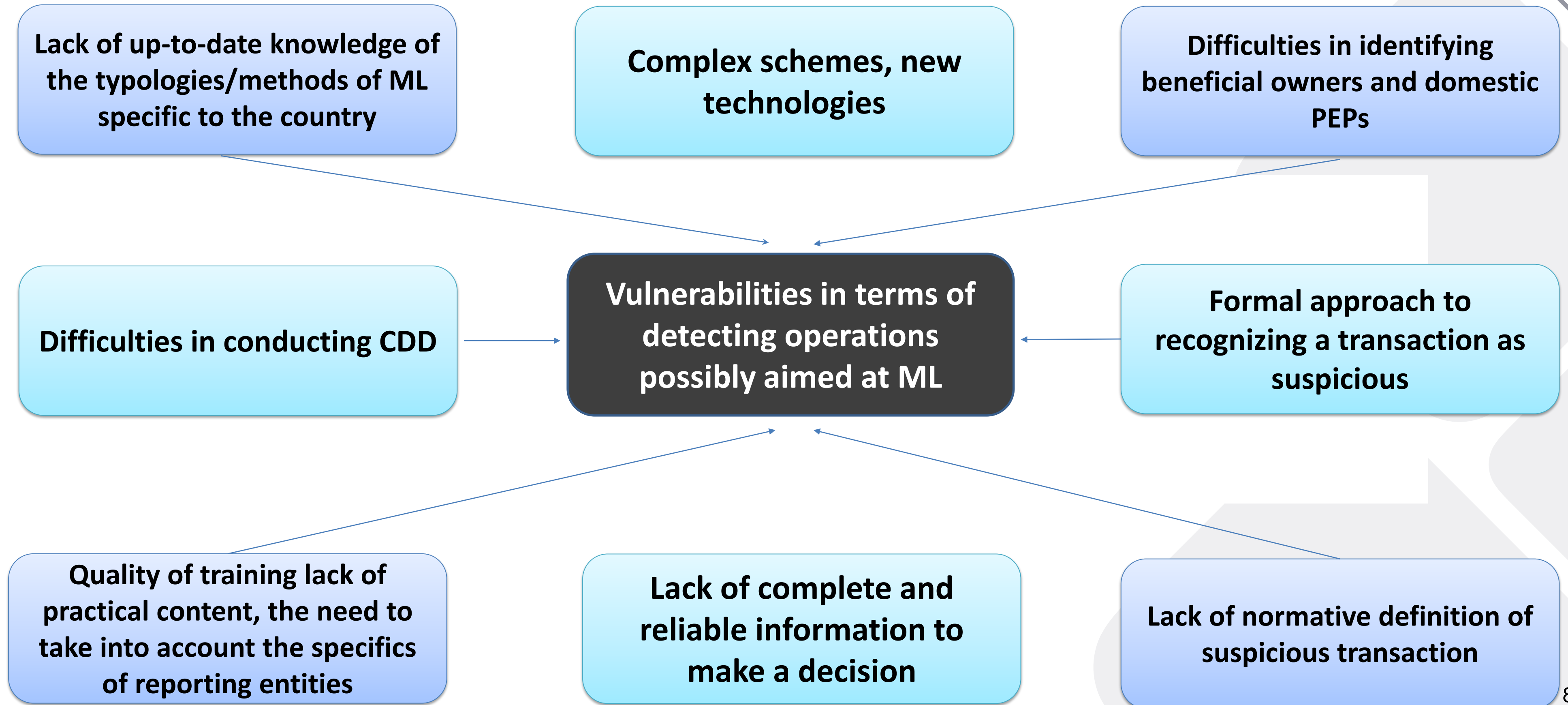
**Introduction of new products and technologies in the financial sector**



**Gaps in the regulation and organization of internal control in the DNFBP and financial sectors**



# Vulnerabilities - organizational factors



# Possible responses to vulnerabilities



As a result of the RRA project, include in technical assistance plans training for DNFBPs and training for all reporting entities on typologies, sanctions lists, and other topics identified by the questionnaire



Involvement of EAG in trainings



Sending information to the private sector by FIU and other competent authorities about relevant ML typologies



Development of a unified methodology for qualifying transactions



Creating a list of positions or a list of domestic PEPs

**Development of a Guidance to clarify the requirements of R.12** (proposal by the representative of Tajikistan)



Development of a methodology for identifying beneficial owners based on typical ownership and control schemes



Raising public awareness of AML/CFT legislation requirements



Any other suggestions?

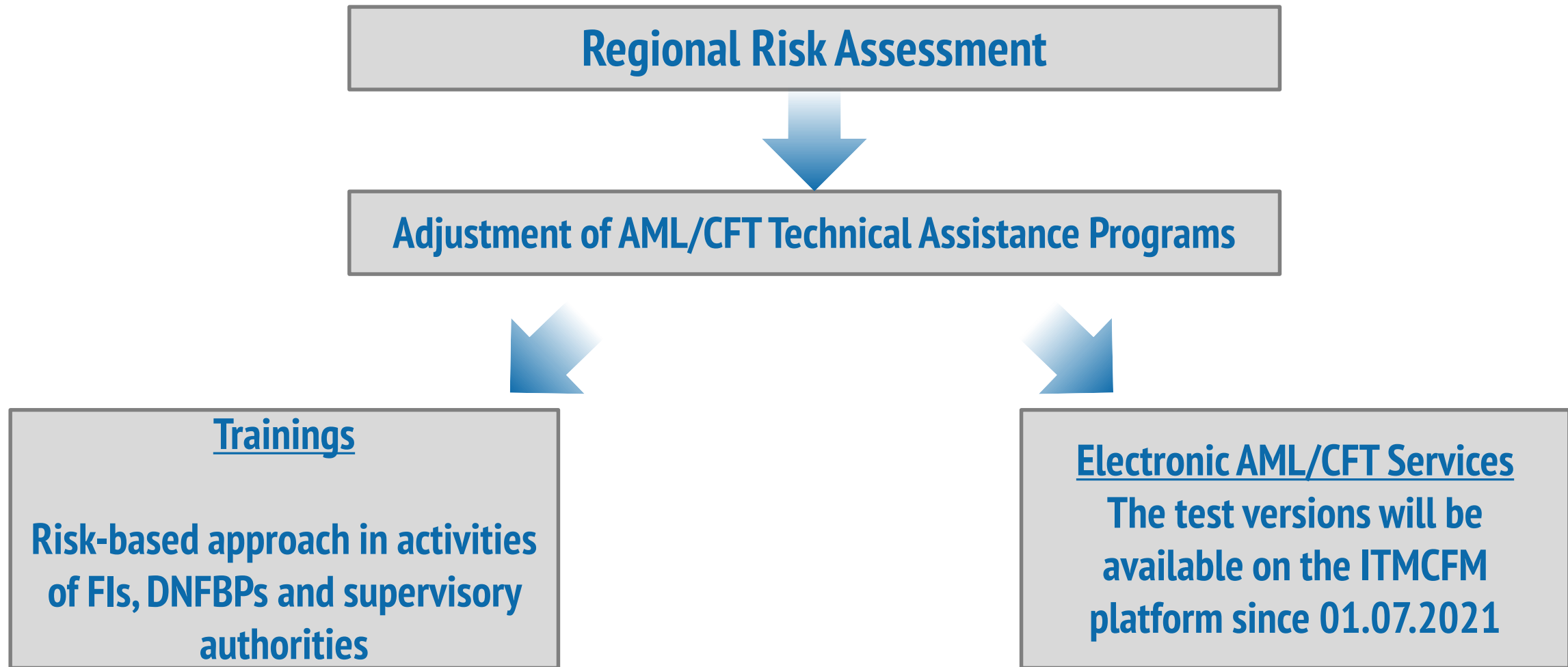


**Thank you for your  
attention!**

# Technical Assistance Projects of the Russian Federation in the Context of Regional ML/TF Risk Assessment

Oleg Ivanov – First Deputy General Director of ITMCFM

# Application of the Regional Risk Assessment Findings



# Electronic AML/CFT Services



- National ML/TF Risk Assessment Center



- Personal Account of an Entity



- Personal Account of Supervisory Authorities



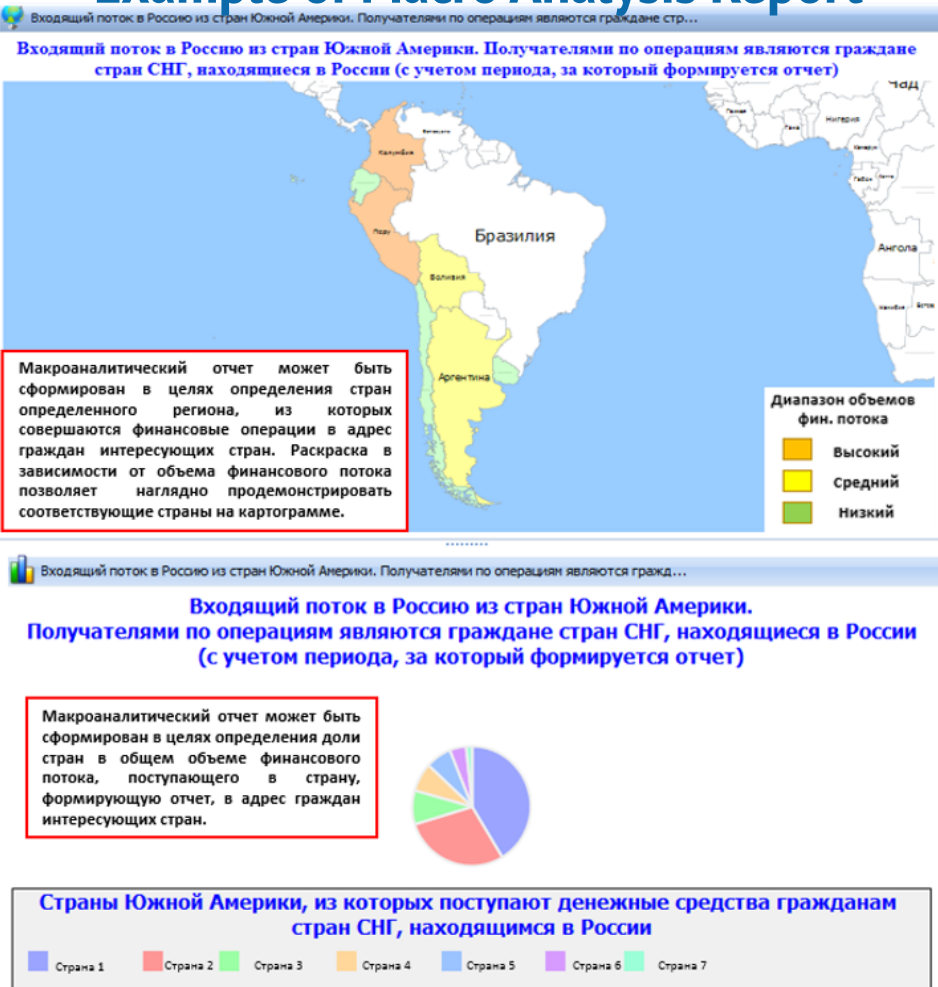
- Transparent Blockchain



- “Graphus” System

# National ML/TF Risk Assessment Center (NRAC)

## Example of Macro Analysis Report

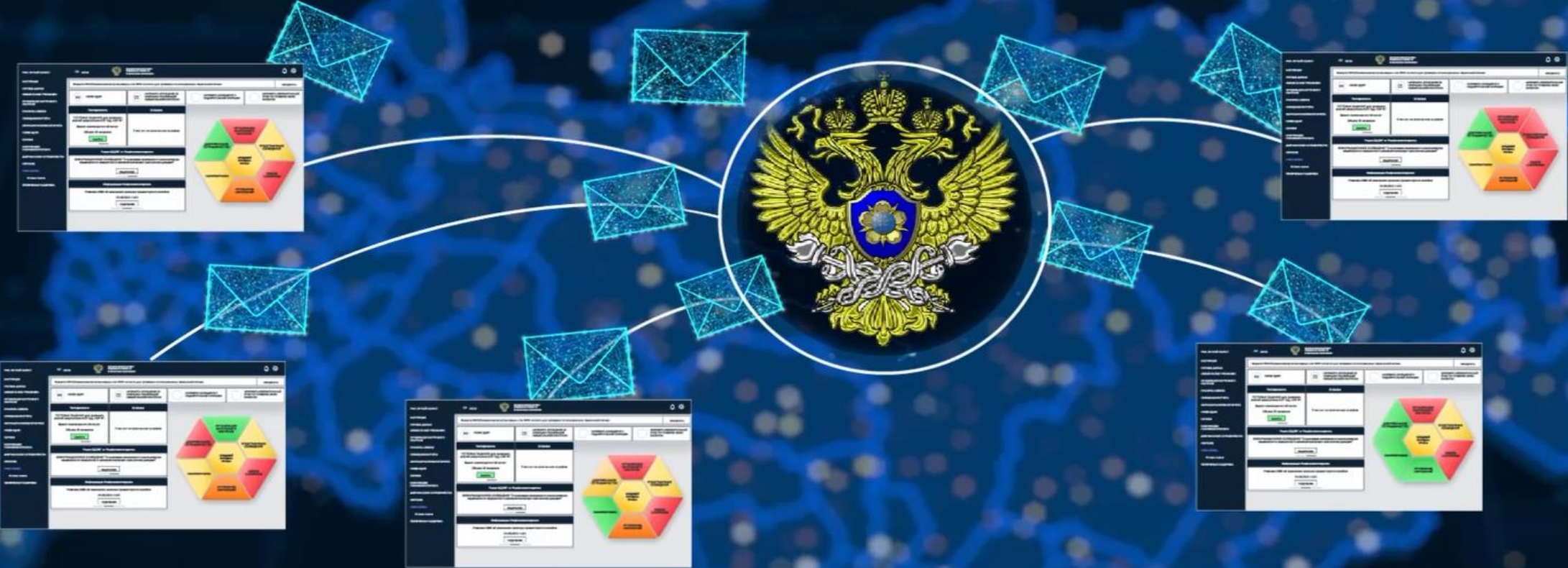


## NRAC Capabilities

- Carrying out multifactorial strategic data analysis
- Identification of tendencies and anomalies
- Financial investigation triggers



# Personal Account of an Entity






# Personal Account of an Entity




МУИЦБМ




# Personal Account of an Entity



**РИСКИ ОД/ФТ**



**АКТУАЛЬНЫЕ  
ТИПОЛОГИИ**



**ИНДИКАТОРАХ  
ПОДОЗРИТЕЛЬНЫХ  
ОПЕРАЦИЙ**

РОСФИММОНИТОРИНГ  
Федеральная служба  
по финансовому мониторингу

Введите ИНН/наименование организации или ФИО клиента для проверки по санкционным перечням/спискам

ПРОВЕРИТЬ

РИСКИ ОД/ФТ

НАПРАВЛить СООБЩЕНИЕ ОБ ОПЕРАЦИИ, ПОДЛЕЖАЩЕЙ ОБЯЗАТЕЛЬНОМУ КОНТРОЛЮ

НАПРАВЛить СООБЩЕНИЕ О ПОДОЗРИТЕЛЬНОЙ ОПЕРАЦИИ

НАПРАВЛить ЕЖЕКВАРТАЛЬНЫЙ ОТЧЕТ ПО ПРОВЕРКЕ СВОИХ КЛИЕНТОВ

Тестирование

ТЕСТОВЫЕ ЗАДАНИЯ для проверки знаний результатов НОР ОД, НОР ФТ  
Время прохождения: 60 минут  
Объем: 18 вопросов  
ПРОЙТИ

Штрафы


У вас нет не оплаченных штрафов

Риски ОД/ФТ от Росфинмониторинга

ИНФОРМАЦИОННОЕ СООБЩЕНИЕ "О признаках возможного использования недвижимого имущества в схемах легализации преступных доходов"  
ПОДРОБНЕЕ

Информация Росфинмониторинга

Решение МВК об изменении размера гуманитарного пособия  
04.08.2020 15:23  
ПОДРОБНЕЕ





- ☒ 140, Организация, оказывающая посреднические услуги при осуществлении сделок купли-продажи недвижимого имущества
- ☐ 160, Оператор по приему платежей
- ☐ 170, Коммерческая организация, заключающая договоры финансирования под уступку денежного требования в качестве финансового агента
- ☐ 999, Иная
- ☐ 998, Вид деятельности не определен
- ☐ 141, Индивидуальный предприниматель, оказывающий посреднические услуги при осуществлении сделок купли-продажи недвижимого имущества



РЕЕСТР ОРГАНИЗАЦИЙ



ИНФОРМАЦИЯ РОСФИНМОНИТОРИНГА



## ПЕРЕЧНИ



РИСКИ ПОД/ФТ



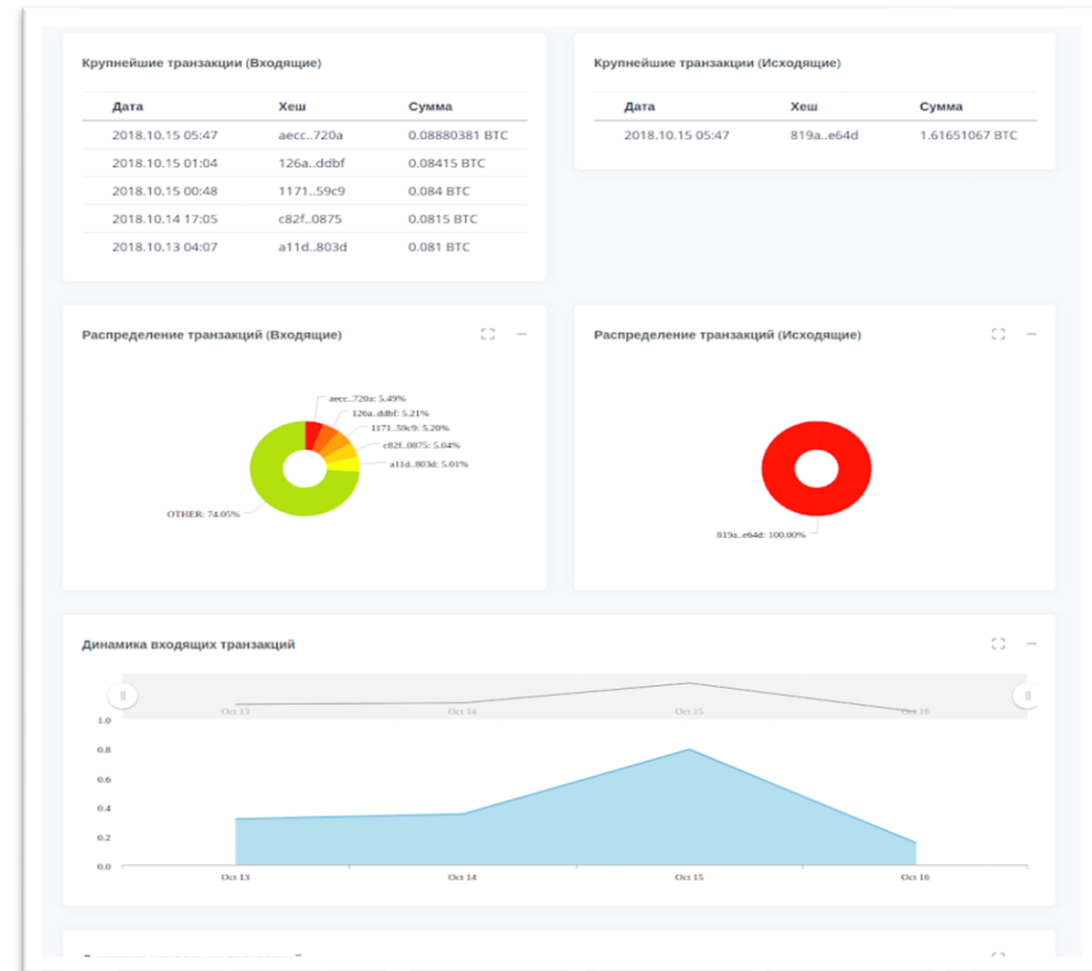
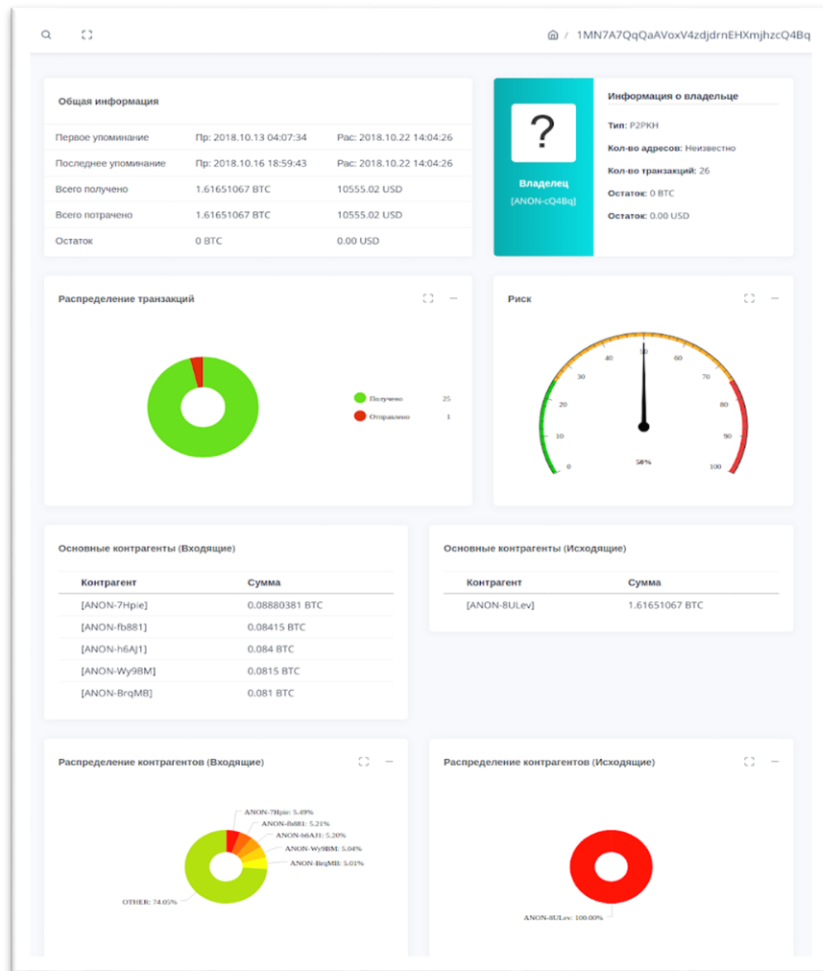
## ОБЯЗАТЕЛЬНЫЕ ТРЕБОВАНИЯ



ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

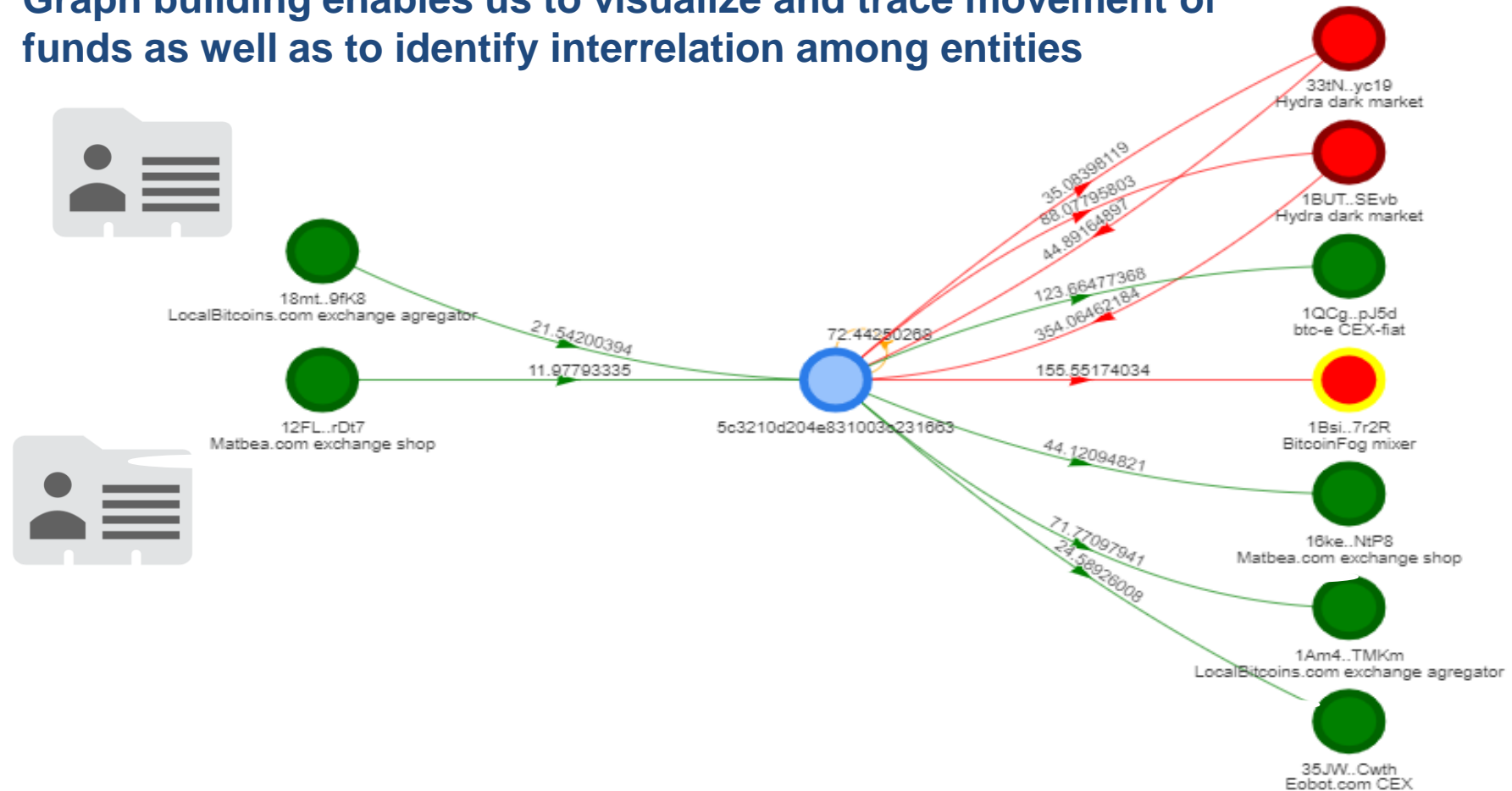


# “Transparent Blockchain” System Interface



# Example of Investigation

Graph building enables us to visualize and trace movement of funds as well as to identify interrelation among entities



# “Graphus” – AML/CFT Financial Investigations Online Training System



Транзакции сговорщиков и лк

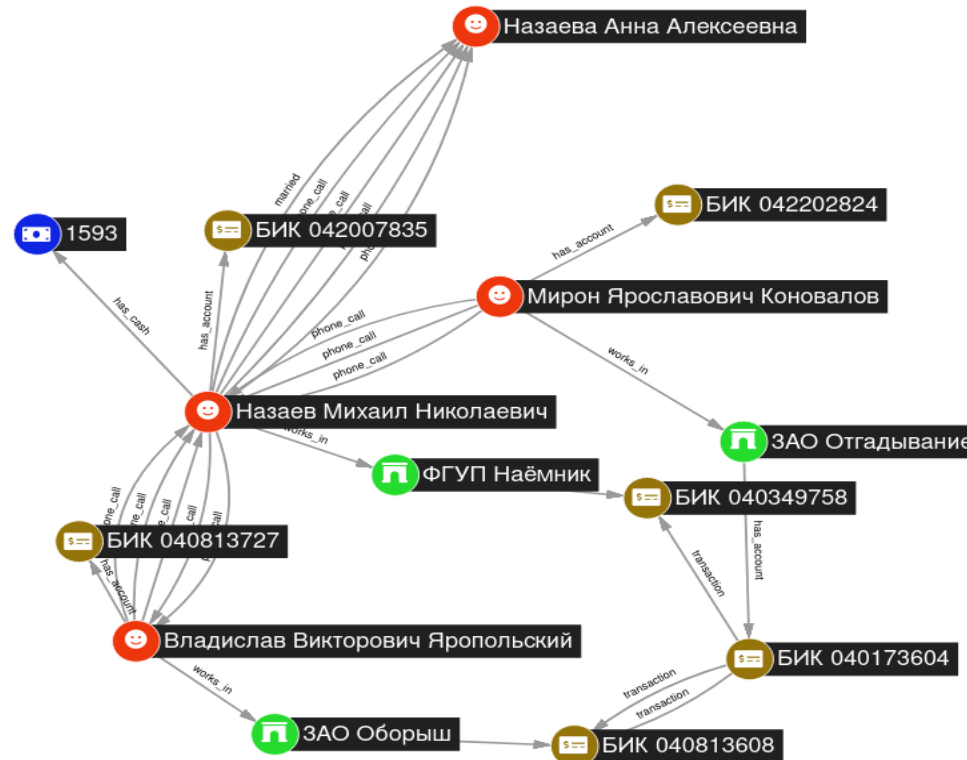
Подграфы Граф



Organization (3) account (6) person (4) cash (1)  
has\_account (6) works\_in (3) transaction (3) has\_cash (1) phone\_call (12) married (1)

Force Сброс

☒ Показать все надписи



# International Financial Security Competition



**Improvement of general information, financial and legal literacy of the youth as well as identification of talented pupils and students in the area of financial security**



**Creation of favorable environment for individual educational trajectories and assisting in development of professional orientation of pupils and students**



**Promotion of learning, cognitive and research activities of pupils and students as well as development of financial security knowledge**

# Competition Schedule

**All-Russian financial security lesson**

**I Stage of the Competition (qualifying)**

**II Stage of the Competition (final)**

## I Stage of the Competition

**Held at the member universities of the International  
Network AML/CFT Institute**

**Participants – 8-10 graders and university students**

**Duration – May 17–21, 2021**

**Winners are qualified for the II Stage of the Competition**

## II Stage of the Competition

**Held at “Sirius” federal territory (Sochi city,  
Russia)**

**Duration – October 3-9, 2021**



**Thank You for Attention!**

# Using RegTech Platforms for Multilevel ML/TF Risk Assessment





# National Risk Assessment Methodology



FATF GUIDANCE

## National Money Laundering and Terrorist Financing Risk Assessment

February 2013



“...while the private sector may not in all countries be an active participant in the national ML/TF assessment, it may be the best source of information in many areas. Contributors from the private sector that may provide essential input to the national-level ML/TF risk assessment process include the following: financial institutions and DNFBPs, industry associations and self-regulatory bodies (SRBs), etc....”

# Survey with the Use of the Personal Account on the Rosfinmonitoring Website



РФМ. ЛИЧНЫЙ КАБИНЕТ ▾

ИНСТРУКЦИИ

УЧЕТНЫЕ ДАННЫЕ

ОБЯЗАТЕЛЬНЫЕ ТРЕБОВАНИЯ

ОРГАНИЗАЦИЯ ВНУТРЕННЕГО КОНТРОЛЯ

ПРОВЕРКА КЛИЕНТА

СООБЩЕНИЯ И ОТЧЁТЫ

ЗАПРОСЫ РОСФИНМОНИТОРИНГА

РИСКИ ОДУ/ФТ

ПЕРЕЧНИ

ИНФОРМАЦИЯ РОСФИНМОНИТОРИНГА

ДОБРОВОЛЬНОЕ СОТРУДНИЧЕСТВО

Опросные листы

Анкетирование

Самодекларирование о неосуществлении деятельности

ОБУЧЕНИЕ

РИСК-ОЦЕНКА

ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

МЕНЮ

РОСФИНМОНИТОРИНГ  
Федеральная служба по  
финансовому мониторингу

100

Горячев Н. А.

АНКЕТИРОВАНИЕ

АНКЕТА: ОПРОС ПО  
ФУНКЦИОНАЛУ ЛИЧНОГО  
КАБИНЕТА  
ВРЕМЯ ВЫПОЛНЕНИЯ: 30  
МИНУТ  
КОЛИЧЕСТВО ВОПРОСОВ: 7

[Посмотреть](#)

commandview	Наименование анкеты	Начало	Окончание	Результат анкетирования
<a href="#">Просмотреть</a>	Опрос по функционалу Личного кабинета	02.07.2020 11:21	02.07.2020 11:51	Анкетирование пройдено
<a href="#">Просмотреть</a>	Опрос по функционалу Личного кабинета	02.07.2020 10:25	02.07.2020 10:55	Анкетирование пройдено
<a href="#">Просмотреть</a>	Опрос по функционалу Личного кабинета	26.06.2018 14:13	26.06.2018 14:43	Анкетирование пройдено
<a href="#">Просмотреть</a>	Опрос по функционалу Личного кабинета	26.06.2018 08:13	26.06.2018 08:43	Анкетирование пройдено
<a href="#">Просмотреть</a>	О предложениях по развитию функционала и интерфейса Личного кабинета (ТЕСТ)	26.06.2018 08:13	26.06.2018 09:13	Анкетирование пройдено

# Real Estate Agents Survey with the Use of the Personal Account on the Rosfinmonitoring website



Questions suggesting the choice of one of the proposed answers

What is the scale of your organization's activities?

What, in your opinion, are the prospects for intermediary activity in the real estate market in the medium term?

How do you think if a criminal will use the services of a real estate agent to purchase/sell real estate objects?

# Real Estate Agents Survey with the Use of the Personal Account on the Rosfinmonitoring website



## Questions suggesting the choice of one of the proposed answers

What is the order of your actions if there are signs of unusual customer behavior, which can be associated with high risks of the particular transaction?

What prevents you from more actively informing Rosfinmonitoring about suspicious transactions (operations) carried out by your clients?

What is the order of your actions if there are attempts by the client to hide the identity of the true participant in the transaction (owner), the person who actually manages the transaction, who is not an official party to the transaction (or a representative of one of the parties to the transaction)?

# Real Estate Agents Survey with the Use of the Personal Account on the Rosfinmonitoring website



Questions involving ranking of answers in the decreasing order of importance on a 5-point scale

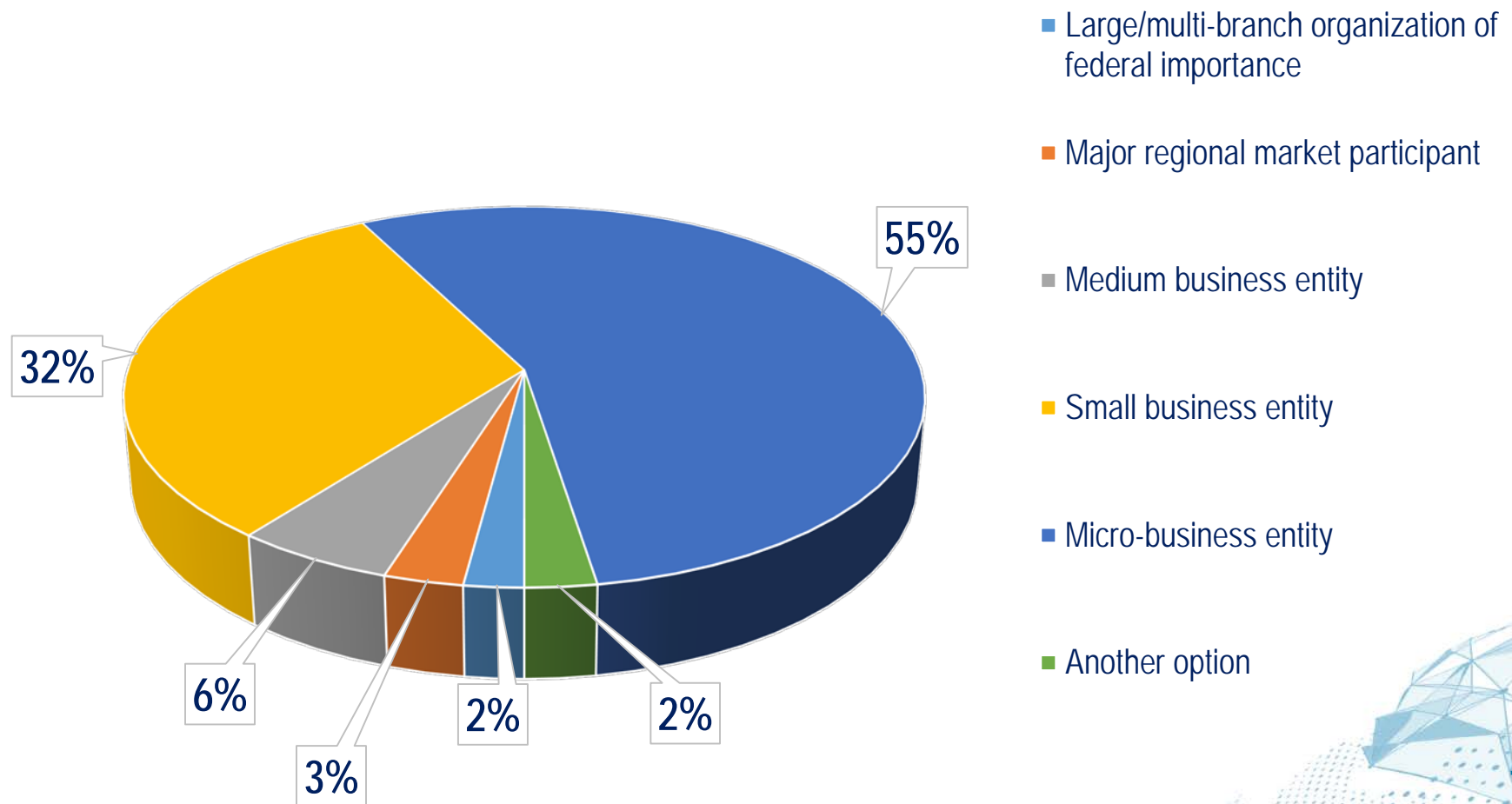
For what reasons, in your opinion, are real estate transactions attractive for money laundering purposes?

	Indicate the rank:
Cash payments	
High cost and high liquidity at the same time	
Opportunity to receive current income (for example, generated from renting)	
Possibilities for manipulating the value of a real estate object	
Possibility for registering a real estate object to a front man	

# Real Estate Agents Survey with the Use of the Personal Account on the Rosfinmonitoring website



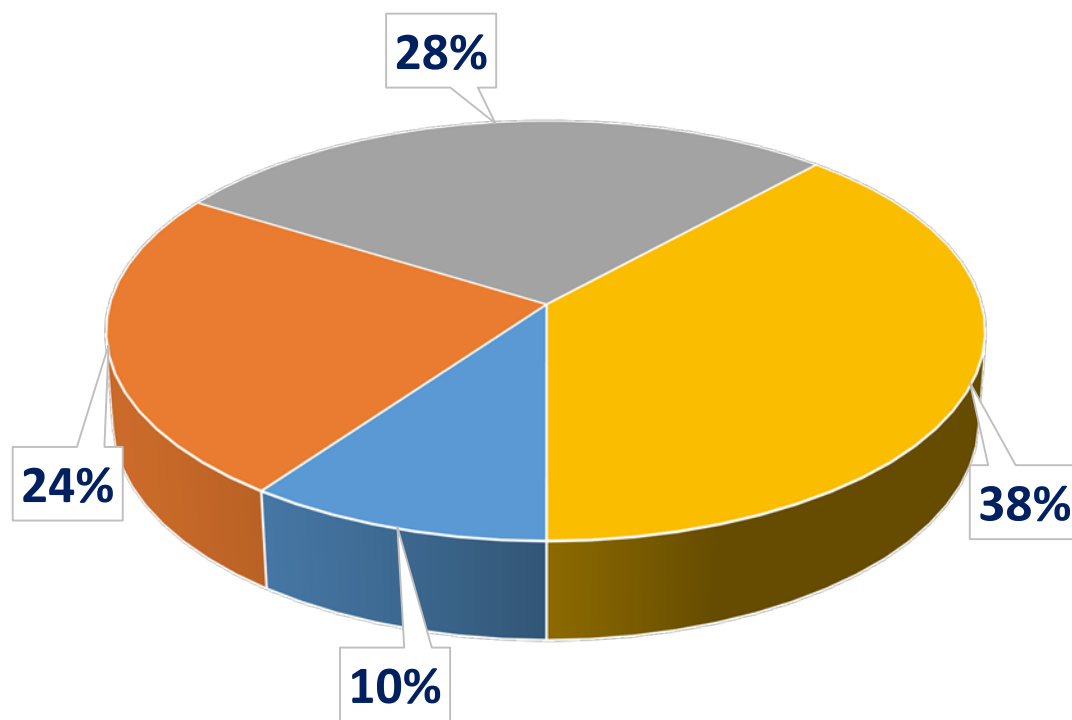
About 1,000 respondents took part in the survey



# Answers to the Real Estate Agents Survey



How do you assess the trends in the intermediary sector of the real estate market:

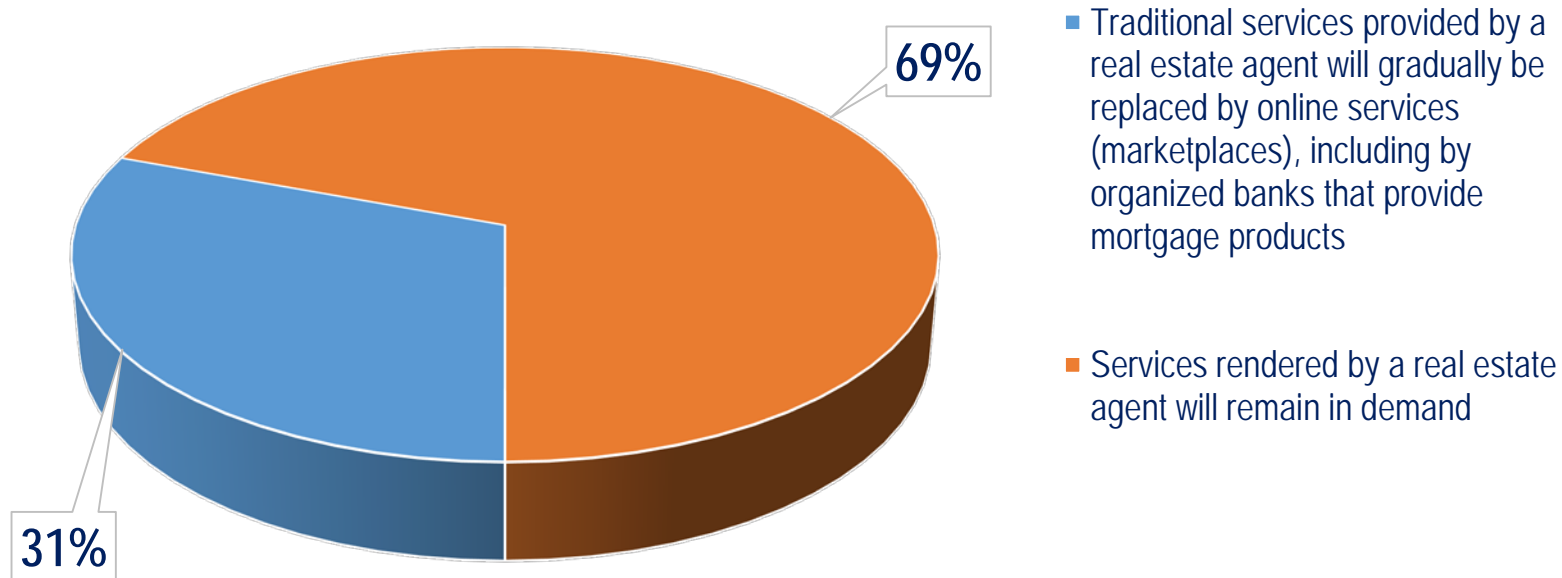


- There is a significant increase in the demand for intermediary services in the real estate market
- There is a slight increase in the demand for intermediary services in the real estate market
- Service demand remains at pre-crisis level
- There is a decrease in the demand for intermediary services in the real estate market

# Answers to the Real Estate Agents Survey



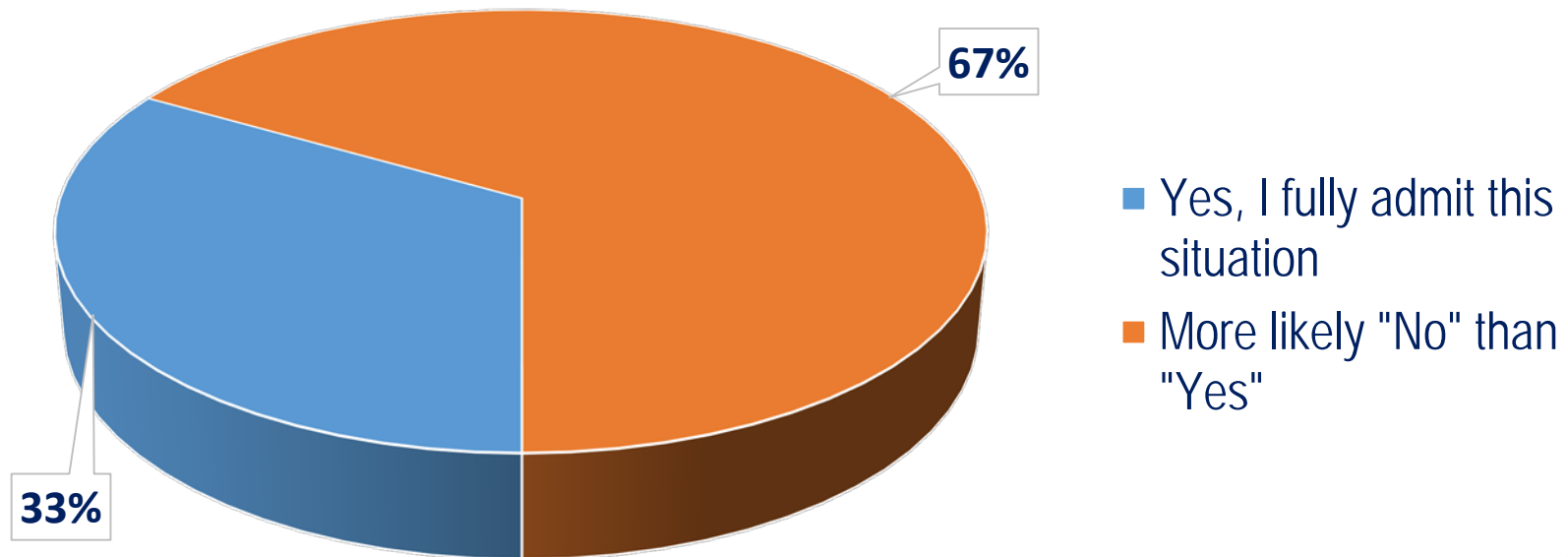
What, in your opinion, are the prospects for intermediary activity in the real estate market in the medium term?







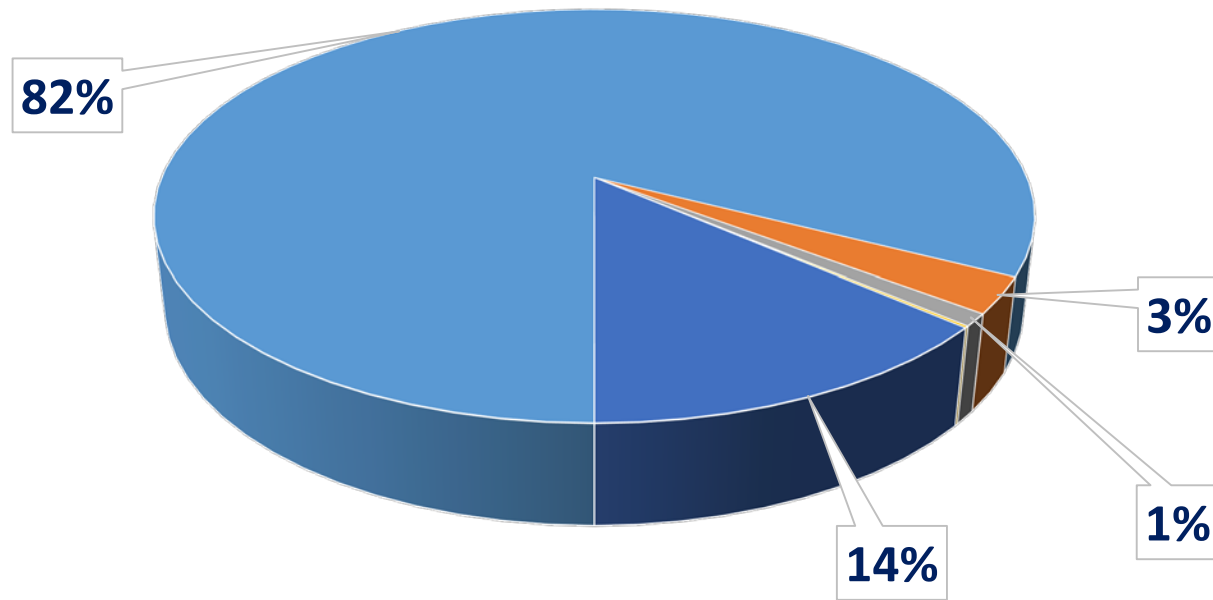
How do you think if a criminal will use the services of a real estate agent to purchase/sell real estate objects?



# Answers to the Real Estate Agents Survey



What is the order of your actions if there are attempts by the client to hide the identity of the true participant in the transaction (owner), the person who actually manages the transaction, who is not an official party to the transaction (or a representative of one of the parties to the transaction)

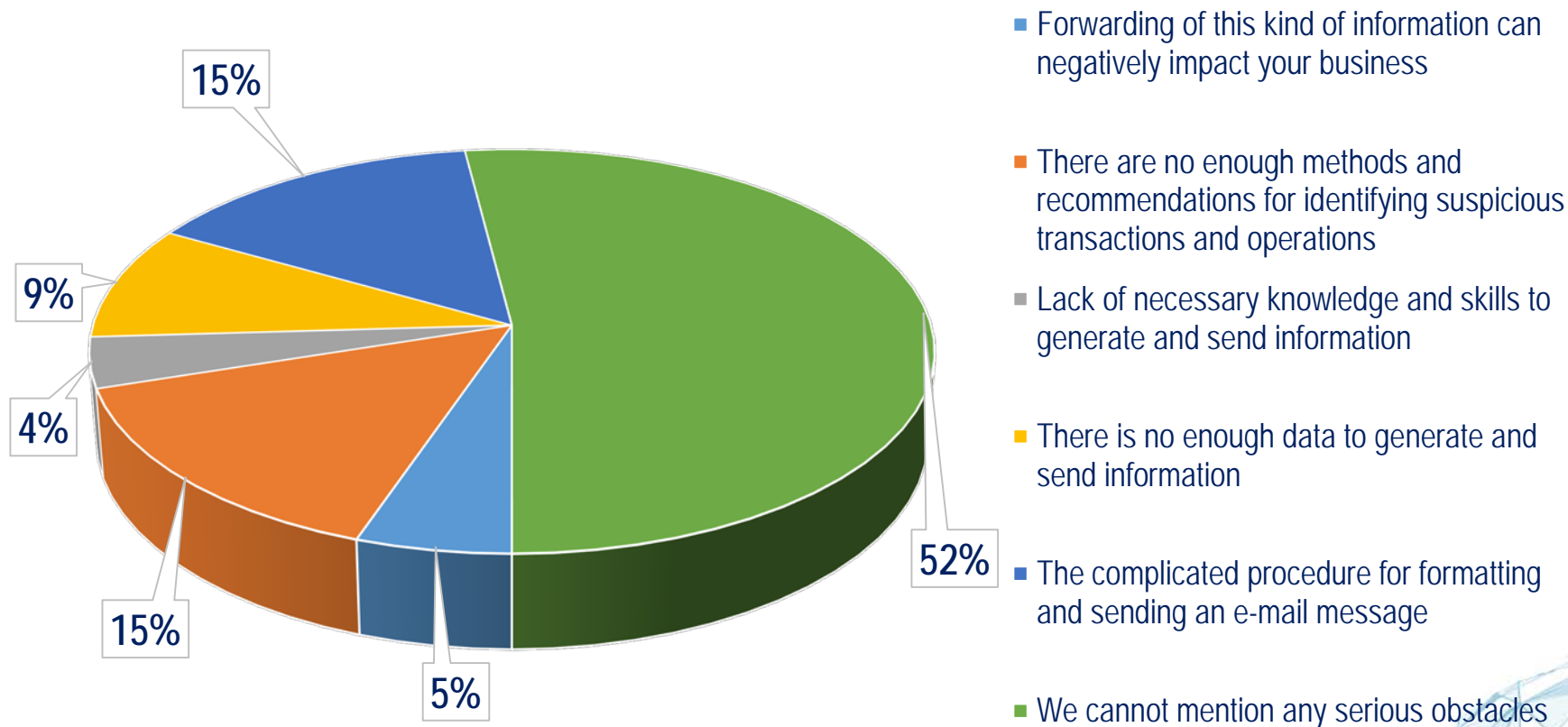


- Such situations occur, and they serve as the basis for requesting additional transaction documents from the client and information on the sources of origin of his/her funds, as well as for forwarding information on a suspicious transaction to the FIU
- Such situations arise, but they do not serve as the basis for assigning a high-level risk to the client.
- As a rule, additional analysis from the standpoint of identifying the true participant in the transaction (owner), the person who actually manages the transaction, is not carried out.
- We do not take any actions, because request of additional information may lead to the loss of the client
- Other (there were no such situations)

# Answers to the Real Estate Agents Survey



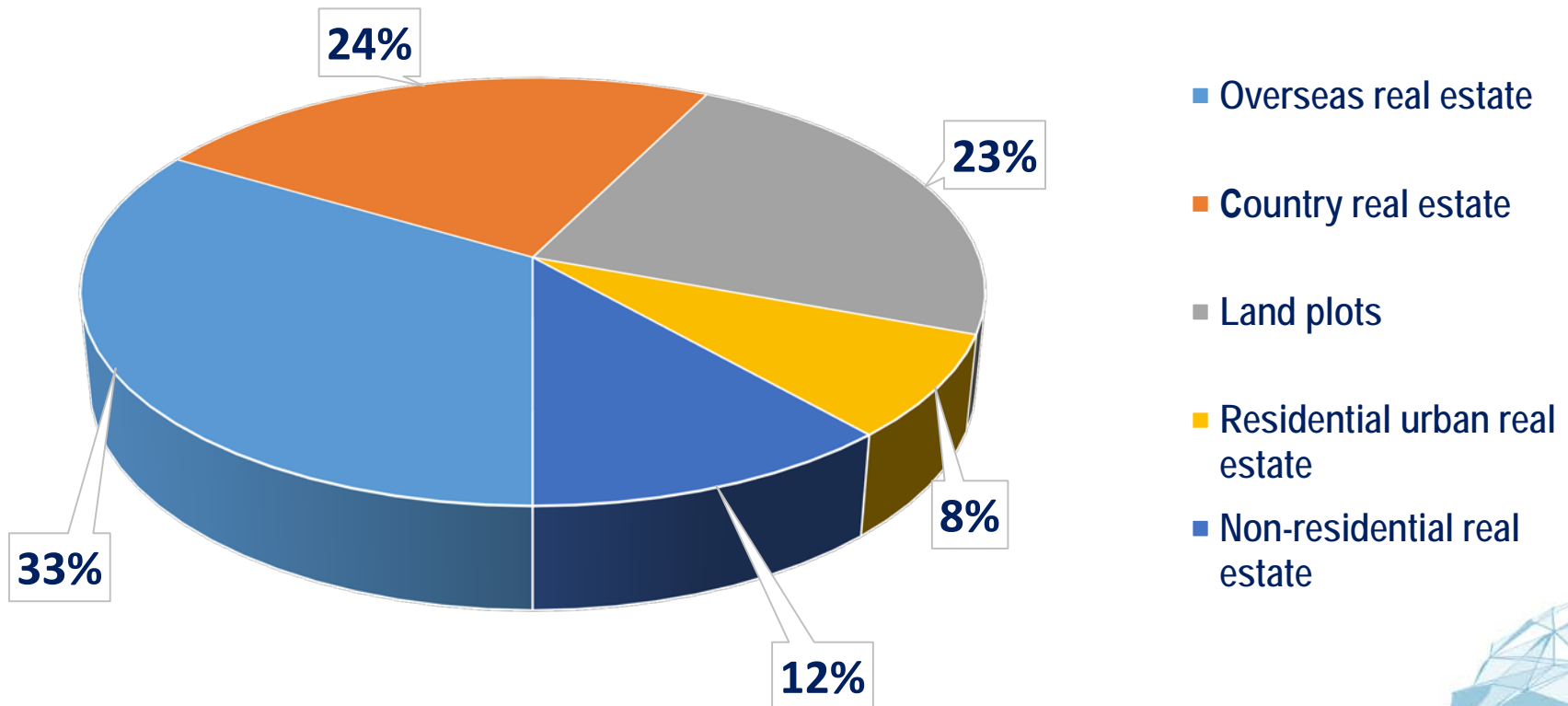
What prevents a real estate agent from actively reporting suspicious transactions?



# Answers to the Real Estate Agents Survey



What real estate objects, in your opinion, are the most attractive for investment of criminal proceeds?



# Use of Survey Results

---



- Conducting sectoral and national ML/TF risk assessment;
- Orientation of real estate agents towards risks and vulnerabilities (feedback);
- Development of an action plan to reduce risks in the sector;
- Preparation of training manuals for universities of the International Network AML/CFT Institute

# Thank you for attention!





# On the AML/CFT situation in the EAG States in relation to the COVID-19 and measures to mitigate ML/TF risks

---

The Eurasian group on combating money laundering and financing of terrorism (EAG)

## **Overall situation in the region caused by the pandemic**

---

Uneven impact of the pandemic on states in the EAG region

Lack of a unified policy

Countries with and without different restrictive regimes

Restrictions imposed on:

- Cross-border movements / mass gatherings of people
- Entrepreneurial activity
- Providing part of the financial services



# The dynamics of predicate offences

## Positive trends

- Reduction of socially dangerous acts and property crimes

## Negative trends

- Increase in fraud, including high-tech and investment fraud
- Cybercrime (phishing, hacking, ransomware)
- Selling/providing illegal health products and services
- Collusion and manipulation of prices for health products and services
- Corruption offences
- Public procurement offences

## The dynamics of predicate offences

### Fraud

- Sale of PPE/ drugs
- Ticket refunds
- Medical tests, physical examinations, tests for COVID-19
- Selling unique products
- Investment fraud / pyramid schemes / shell companies
- Tax refunds
- Receipt of benefits/ rebates
- Purchase of movement permits during restrictions
- Transferring funds for treatment
- Mock mailings on behalf of the World Health Organization / mock mailings from charities, World Bank or IMF charitable campaigns

## **New vulnerabilities due to COVID-19**

---

Increasing customer dependency on transactions made through online channels

allocation of subsidies/ lending funds by governments on the basis of misguided/ false targets

the periodic deterioration of the client profile due to absence of physical presence;

an increase of cash transactions

restrictions on carrying out AML\CFT inspections

deterioration of the economic situation in the country

# Measures taken to mitigate the impact of the COVID-19 pandemic

---

Regulatory measures

Measures taken by FIUs

Law enforcement measures

Supervisory measures

Measures taken by financial institutions

## Regulatory mitigating measures

---

Establishment of a legal and regulatory framework for receiving public services remotely

Establishment of a legal and regulatory framework for remote access to the financial institutions services

Expanding the requirements of Basic AML/CFT laws

Information dissemination for reporting entities

## FIU mitigating measures

---

The FIU informs the private sector about the threat of COVID-19, associated risks and typologies

Monitoring of open-source information for fraud schemes related to COVID-19

Additional monitoring of the medical companies

Additional analysis of STRs with specific attributes

## **Law enforcement authorities mitigating measures**

---

Disseminating information about relevant risks and fraud schemes

Media relations

Building a system of remote communication with citizens

There is ongoing monitoring of the spending of the budget allocated to preventing the effects of COVID-19

Permanent monitoring of the government contracts related to COVID-19



## **Supervisory bodies mitigating measures**

---

Changes in the format of inspections and the format of engagement with the private sector

Prompt communication of the typologies and risks associated with the epidemic situation, signs (indicators) of suspicious operations

Introduction of a dedicated coronavirus-related STR indicator

Measures to encourage online payments

Relaxation of regulatory requirements

**Thank you for your  
attention**

**UKNF**

URZĄD  
KOMISJI  
NADZORU  
FINANSOWEGO

**Paweł Paluszyński**

Compliance Department

2021.04.29

**Supervisory initiatives  
taken by the Polish  
Financial Supervision  
Authority to mitigate the  
risk of money laundering  
and financing of terrorism  
in Poland in the time of  
the COVID-19 pandemic**

# The Polish Financial Supervision Authority

The Polish Financial Supervision Authority (the UKNF) was established in September 2006.

The mission of the UKNF is to ensure stability and safe development of the financial market.

The UKNF is an independent body, whose tasks are aiming to limit excessive risk in the operation of supervised entities (not only limited to risks related to money laundering and financing of terrorism – ML/FT) and strengthen the transparency of the financial market.

The UKNF exercises supervision over the:

- banking sector,
- capital market,
- insurance market,
- payment institutions and payment service offices,
- electronic money institutions,
- the cooperative credit union sector.

# New Risks Related to COVID-19

The coronavirus pandemic (COVID-19) has created new challenges for the financial institutions and the authorities responsible for combating money laundering and financing of terrorism.

Among the identified new risks and trends, the most significant ones are:

- Establishing business relationships without a physical presence of the customer – „remote” identification and verification of the customer, usually through the Internet.
- New fraud schemes, such as:
  - scams involving medicines or personal protective equipment,
  - social media scams and telephone calls fraudulently asking for donations for illegitimate charities,
  - telephone calls by individuals pretending to be government officials asking for personal information or bank account information,
  - fake investment companies promising high returns (this type of fraudulent activity has recently increased significantly in Poland).

# The Initiatives Taken by the Polish Financial Supervision Authority to Mitigate Risk

The UKNF has taken actions in order to mitigate new types of risks and to increase the security of the financial market in Poland. The key initiatives are as follows:

- In 2019 the UKNF published an official statement on customer identity verification through video verification means. This document sets out good practices related to verification of identity of customers who are not physically present for identification purposes.
- In 2020 the UKNF published a questionnaire form to be used by banks in relation to payment institutions. The main goal of the above-mentioned questionnaire is to guarantee the security of financial transactions and proper fulfilment of the requirements under the Polish AML/CFT Act by supervised entities.

# The Initiatives of the Polish Financial Supervision Authority

- In 2020 the UKNF issued guidelines on the money laundering and terrorist financing risk self-assessment of supervised entities – which is one of the obligations under the Polish AML/CFT Act and Directive (EU) 2015/849 of the European Parliament and of the Council – the so called the 4th AML Directive.
- The UKNF is concerned about new trends related to frauds, especially linked to fake investment schemes, which have significantly increased in Poland recently.



Inability to meet the customer „physically” may affect a financial institution’s ability to properly identify and verify its customers and consequently to conduct an effective customer risk assessment. The key risk factors related to establishing business relationship „remotely” are as follows:

- Before the pandemic, the Know Your Customer (KYC) processes usually required the customer to verify his/her identity „physically” at a financial institution’s branch. The new circumstances forced financial institutions to quickly change their approach and introduce new distribution channels (the Internet) without carrying out proper risk assessment and implementing adequate tools or procedures.
- The costs of dedicated tools which could be used for establishing business relationship remotely are overwhelming for smaller institutions (e.g. payment service offices).
- The identity verification process often relies on photocopies of identification documents provided by potential customers, which makes checking the authenticity of documents much more difficult.

The above-mentioned factors often lead to oversimplification of the KYC processes and, as a consequence, to applying inadequate due diligence measures towards „remote” customers.

Payment accounts offered by payments institutions are often used by criminals to commit frauds or for money laundering activity. The main reasons for that are as follow:

- limited awareness about the potential ML/FT risks,
- shortage of dedicated tools supporting the AML/CFT processes,
- a relatively high level of ML/FT-related risks that payment institutions are willing to accept,
- often simplified KYC processes and procedures,
- close ties with cryptocurrency exchanges.

To ensure the security of financial transactions, the UKNF has taken actions aimed at improving cooperation between banks and the payment services sector. Based on the surveys and experiences gained during inspections, a questionnaire has been prepared, which is based on the questionnaire of the Wolfsberg Group.

- The questionnaire is supposed to facilitate obtaining information about a customer from the payment sector.
- Based on the information provided by payment institutions within the questionnaire, banks can easier identify the ML/FT risk arising from particular business relationship and apply appropriate customer due diligence measures to mitigate that risk.

# ML/FT Risk Self-Assessment of the Obligated Institutions (1)

The requirement to perform the institution's risk assessment is laid down in the Polish AML/CFT Act and follows from the provisions of the 4th AML Directive.

Risk self-assessment represents the key document which determines the measures taken by financial institutions to counter money laundering and financing of terrorism and serves as a starting point for the development of internal AML/CFT processes.

Also, risk self-assessment materially affects:

- the obliged institution's awareness of its exposure to risk, thus its risk appetite,
- the form of internal documents governing the area of AML/CFT at the obliged institution,
- the scope and method of applying financial security measures to the obliged institution's customers,
- the practical approach to the fulfilment of AML/CFT requirements by the obliged institution,
- the measures taken by the obliged institution to mitigate risk in various areas of its business which are particularly exposed to the risks of money laundering and terrorist financing.

# ML/FT Risk Self-Assessment of the Obligated Institutions (2)

Financial institutions are required to update their risk self-assessment in the case of changes in the risk factors related to customers, countries or geographical regions, products, services, transactions or delivery channels. The UKNF expects that the obliged institutions will also consider updating the risk assessment in the case of material long-term changes in the business environment which may have a material impact on the institution's operating activities and the way its products and services are used.

An important example of the above-mentioned circumstance is the epidemic, which has a long-term impact on:

- ML/FT risk exposure of the financial institutions,
- ML/FT risk exposure of the entire financial sector, both in Poland and in the world.

The ML/FT risk self-assessment should serve as a starting point when defining the appetite for the ML/TF risk and when making strategic AML/CFT-related business decisions.

Therefore, in order to properly understand and mitigate the ML/FT risks, it is of vital importance for financial institutions to assess the new factors, like the epidemic or launching new distribution channels, and to update risk self-assessments accordingly.

Fraudulent activity in Poland has recently increased significantly recently. The main reasons behind it are:

- The pandemic forced people to execute transactions remotely (e.g. through the Internet), which limited the possibility to interact with the customer and to inform him/her on potential risks related to his/her transactions.
- The economic environment (relatively high inflation rate, low interest rates) can encourage investors to take more risk in a search for new types of investments and opportunities.
- Currently, one of the most popular fraud schemes is investment scam. Agents of fake investment firms contact their victims directly and offer extremely profitable investments which are only possible through their companies. They often try to persuade their „customers” to reveal bank account information or to install third-party applications allowing them to log into victims’ bank accounts. The invested funds are rapidly moved through several bank or payment accounts and ultimately transferred to anonymous cryptocurrency wallets and disappear.

# Building Awareness of the Financial Market

Every year the UKNF carries out educational activities within the CEDUR (Education Centre for Market Participants) cycle of meetings with representatives of the financial market.

The topic of prevention of money laundering and terrorist financing represents a constant element of training sessions, during which issues related to the ML/TF risk are discussed and the results of inspections and related market practices are presented.

The CEDUR seminars are a perfect opportunity to discuss new risks and identified trends and to share experience between financial institutions and the UKNF representatives.

Training activities bring direct effects. During the inspections of the supervised entities which participated in the CEDUR seminars, the entities often demonstrate that the actions have already been taken in order to fulfill AML/CFT-related obligations in a manner presented during the seminars.

# Thank you!

**Paweł Paluszyński**

**Compliance Department**

pawel.paluszynski@knf.gov.pl

ul. Piękna 20, 00-549 Warszawa

**[www.knf.gov.pl](http://www.knf.gov.pl)**



# Creation of «Know your customer» procedures in the pandemic and digital transformation of services

2021 year

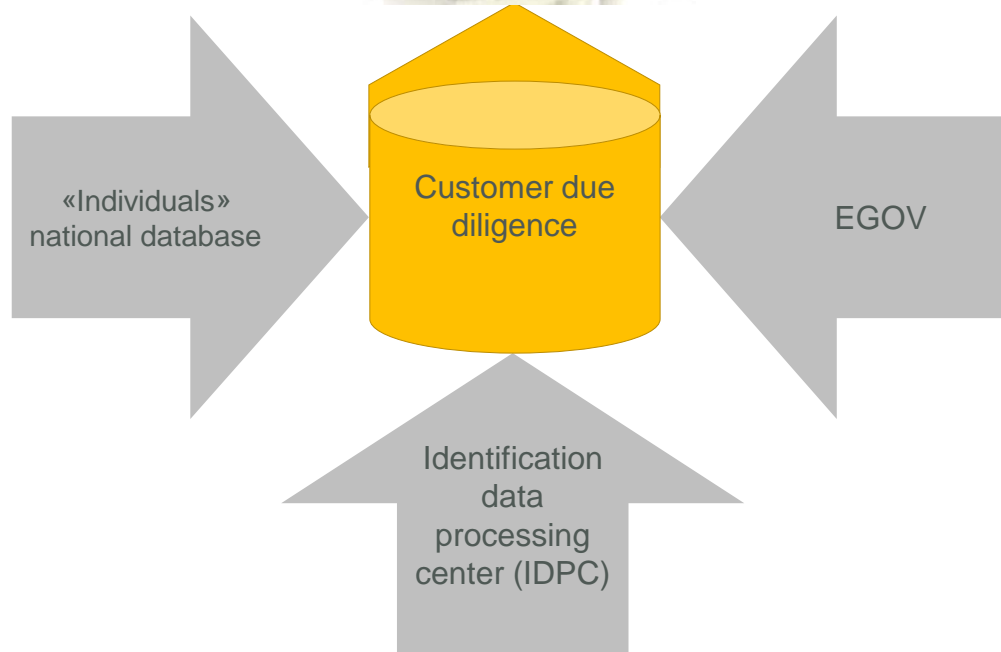
[halykbank.kz](https://halykbank.kz)



[facebook.com/halykbank](https://facebook.com/halykbank)



# Building remote business relationships



Due to the pandemic caused by COVID-19 second tier banks (further - STBs) in 2020 allocated all resources to provide services and products that allow establish business relationships and serve customers remotely.

The legislative framework of the Republic of Kazakhstan (further - RK) including the changes to the Law of the RK on AML/CFT\* and subsidiary legislation\*\*, allows to establish business relationships remotely.

STBs now have the opportunity to verify clients' identification data using provided access to the following state databases: Identification data exchange center (IDEC), «Individuals» national database and the Egov service.

Within the framework of the circumstances associated with the pandemic and the provided technical/legislative opportunities, in 2020 JSC Halyk Bank of Kazakhstan (further - the Bank) implemented service that allows to individual entrepreneurs open account remotely.

The Bank has implemented the procedures for remote establishment of relationships in compliance with all the AML/CFT legislation of the RK requirements and the "Know Your Client" procedures.

\* Anti-money laundering (AML) and counter terrorist financing (CFT) Law of the Republic of Kazakhstan.

\*\* Resolution of the Board of the National Bank of the Republic of Kazakhstan dated June 29, 2018 No. 140 «On approval of the Requirements for clients due diligence in case of remote establishment of business relationships by financial monitoring entities».

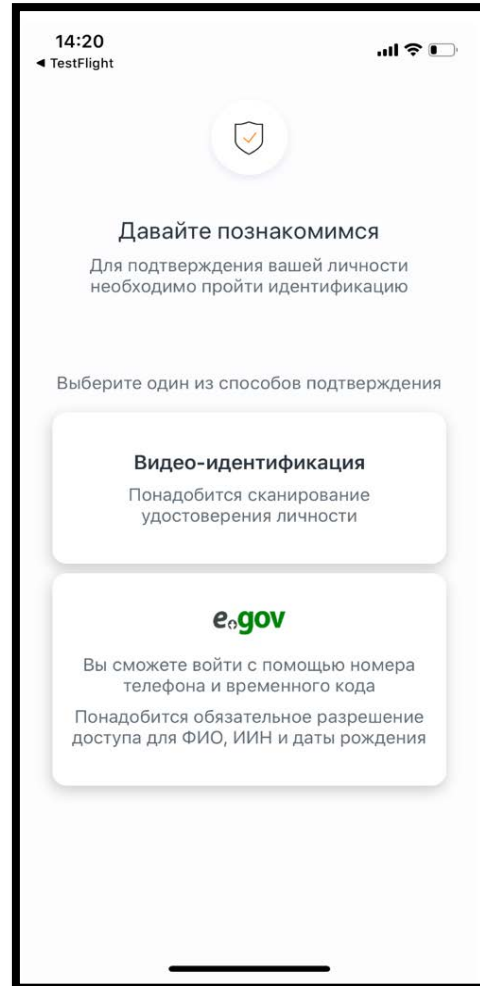
# Client identification and verification of the client's identity through biometrics

*During identification and authentication of clients in the "Onlinebank" remote channel, biometric identification means are used*

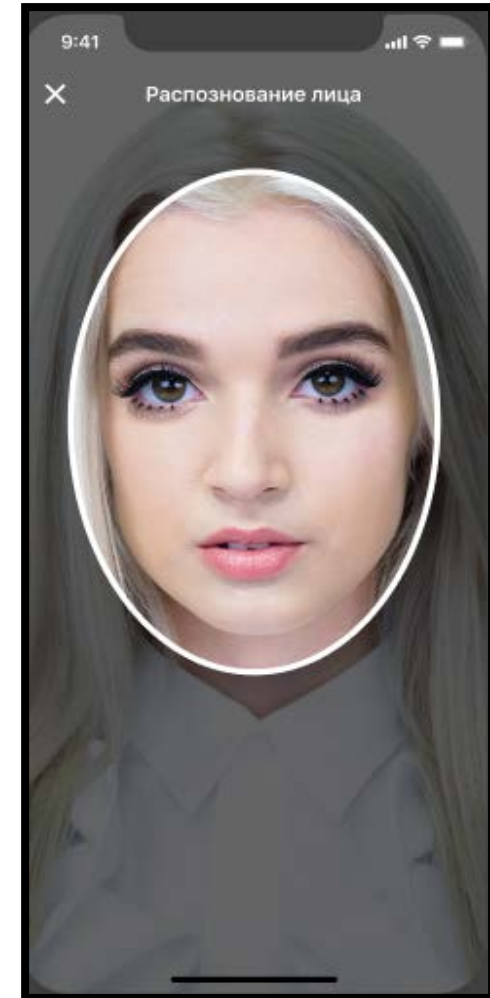


- ✓ Due to KYC procedures the client has to confirm his/her identity (pass identification process)
- ✓ On this stage client can choose how to confirm his/her identity:
  - through the EGOV service
  - through the video identification (state ID card must be prepared)

Thus, clients have two options for identify confirmation, through state portal or through identification in Bank's system.



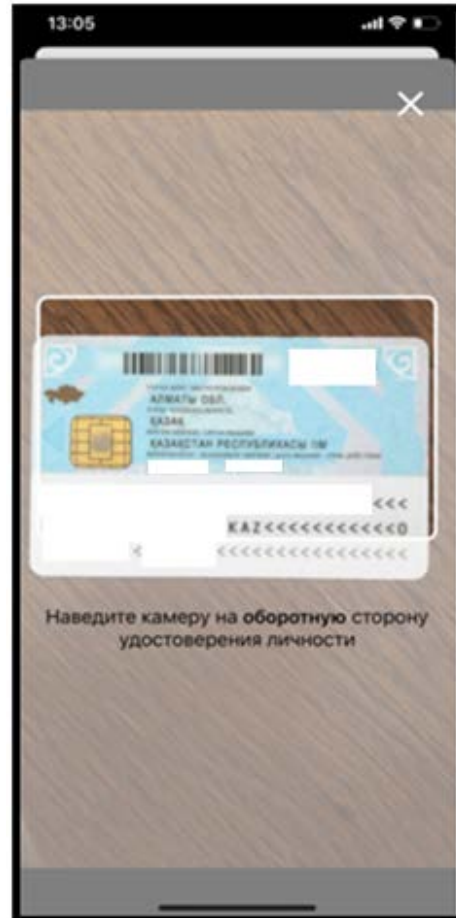
- ✓ In case of video identification in the Bank's system, the client's biometric data is verified with the data available in the Bank and IDEC. Identity verification is carried out using the state database.
- ✓ Video identification must be carried out only by the account owner.



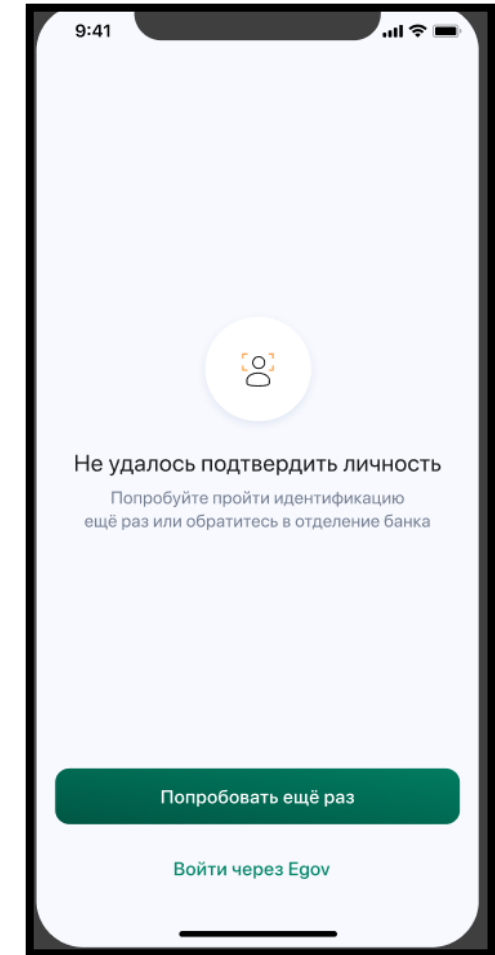
## Client identification and confirmation of the client's identity through biometrics

*During the identification and authentication of clients, the identity of an individual is confirmed by verification with the state databases*

- ✓ In addition to the video confirmation of the client's identity through Individuals national database (INDB) the client's identification data is also verified with information in the scanned state ID card.
- ✓ Confirmation of the client's identity can be done by video identification and verification of the state ID card parameters with the data of state databases.



- ✓ Taking into account the established checks for identity verification and identification all controls must be in place.
- ✓ In case if client's identify confirmation is failed there are a possibility to repeat a video confirmation or confirm it using EGOV portal service.



*It should be noted, that in addition to identity data, the Bank also reconciles the data of the individual entrepreneur/farm owner, with whom the account is opened and establishment of business relationships are built.*

# Restrictions on Remote Establishment of Business Relationships



The Bank establishes business relationships remotely exclusively with customers who meet the following requirements:

- 1) An individual who has been assigned an identification number;
- 2) The client is not a person, included in the list of organizations and persons associated with the financing of terrorism and extremism;
- 3) The client is not a person or organization that is subject to international sanctions (embargo) in accordance with the resolutions of the United Nations Security Council;
- 4) The client is not a person who has been assigned a risk level requiring the application of enhanced due diligence measures in accordance with paragraph 7 of Article 5 of the AML Law and internal control rules.

The Bank decides to establish the business relationships with clients remotely based on the ML / FT risk assessment by the type of client, country (geographic) risk, of the service (product) risk and it's delivery method.

The Bank does not establish business relationships remotely and does not execute transactions in case of:

- 1) non-compliance of the client with the requirements listed above;
- 2) lack of the client's (individual) consent for the collection, processing, storage and disclosure to third parties of his (her) personal data confirmed by the identification tool in case if the client didn't enter his individual number in the remote access system, client's identification and authentication and fixing client information are not performed.
- 3) if the Bank has suspicions that the client is conducting an transactions for ML / FT purposes;
- 4) for other reasons outlined by the Code of the Republic of Kazakhstan «On Taxes and Other Mandatory Payments to the Budget», Law on AML/CFT, Legislation of the Republic of Kazakhstan «On payments and payment systems»

# Remote business opportunities

Realization of product through building remote business relationships allowed:

1

exclude visits of customers in the Bank's local branches and minimize physical contact in a time of a pandemic;

2

reduce the account opening time, provide to clients a possibility to execute transactions (taking into consideration established restrictions), as well as the usage of channel to receive lending products;

3

to carry out the KYC procedure remotely in compliance with all the requirements of the Normative legal acts of the Republic of Kazakhstan and Bank's internal control rules.



# Compliance during the period of new challenges

Timur Mussin | MBA, CAMS

2021





**The World has  
changed a lot..**

## COVID-19

### **Influence of sanitary and epidemiological conditions:**

- increased use of remote channels
- growth in the number transactions
- growth of the social role of the financial sector
- strength testing of continuity processes  
(lack of resources, IT, simplicity of processes)
- the transition of most workers to teleworking
- possible decline in compliance
- frequency and quality of inspections

## ADAPTATION

**Banks and other financial organizations carried out the following activities:**

- reduction in the number of working hours/days
- development of infrastructure for remote work
- training employees in new rules of the game
- care of employees (social programs, division into groups, treatment of premises, masks)
- constant feedback
- simplification of processes (internal and external)
- active change/business development (remote sales channels, new products/services)

**Business is actively changing...**







**Compliance must  
be ready**

## NEW CHALLENGES

**The pandemic has impacted compliance activities:**

- verification of the strength of compliance processes (lack of sufficient resources and tools)
- a sharp change in the business profile of customers
- new schemes of money laundering and an increase in the number of suspicious transactions related to corruption, money laundering and the use of cryptocurrency. Fraud and cybercrime
- risk of information disclosure (laid-off workers, Data loss of telecommuting workers, services with limitations)
- insufficient fulfillment of regulatory requirements in terms of the timeliness of providing information to state bodies
- bringing activities in line with new requirements



**What needs  
to be done?**

## BASIC STEPS

### **Compliance must be ensured:**

- close interaction with business
- active participation in the approval and testing of new services and sales channels
- moving away from “paper compliance” towards developing a compliance culture and using Whistleblowers
- work with employees (constant communication through internal social networks, training, tone from the top)
- empowerment of compliance
- increasing the frequency of interaction with the management board and the board of directors
- timely reporting and responses
- establishing effective interaction with government agencies
- maintaining a sufficient level of compliance in subsidiaries, especially in terms of AML/CFT (functionality, personnel. training)

A man in a dark suit and blue shirt is pulling open his jacket, revealing a bright red shirt underneath. The image is cropped to focus on the chest and hands.

**Who if not us?**

## BASIC STEPS

### **Compliance must be ensured:**

- reorientation of scheduled inspections of high-risk areas
- automation of compliance and AML/CFT processes (reduction of manual labor in order to strengthen analytics, automatic scripts, conclusions, checks)
- improvement of the intrabank AML/CFT typology based on the experience of our own and international
- developing new skills and increasing the versatility of compliance workers
- strengthening processes of Know Your Employee
- participation in events held by HR
- optimization of internal compliance processes, increases mobility



**THANK YOU FOR ATTENTION!**

[mussintimur@mail.ru](mailto:mussintimur@mail.ru)  
[www.linkedin.com/in/faceman/](https://www.linkedin.com/in/faceman/)



# AML practice to reduce ML/FT risks in corporates on-boarding process.

Minsk  
April 29, 2021

## 1. February 20. The main risk of COVID-19, which we expected.

- Involvement customers (corporates, sole proprietors) from business areas that were most seriously affected or could have suffered from the economic downturn due to the COVID-19 in "gray" ML/FT activities.

## 2. AML control measures that were developed earlier and used now.

- ✓ Compliance preliminary on-boarding approval for corporates, sole proprietors related to
  - business areas: gambling, financial services (leasing, insurance, funds, forex, payment service providers, etc.);
  - HR countries (offshore zones, FATF list, including "enhanced monitoring") - customers, founders, managers, BOs registration/citizenship/location analyse;
  - non-resident;
  - non-profit organisations.
- ✓ Plausibility compliance check of the customer relationship 6 months after account opening.
- ✓ Transaction monitoring process (special attention: turnover increasing, dividends, personal income payments).
- ✓ Local managers special attention ("Know your customers") to an activity subject changing, changing the founders to new ones (related to the HR countries).

## 3. 2021 findings.

- General trend: the number of sole proprietors financial transactions related to personal income withdrawing or transfer to cards has increased (the subject of AML monitoring).

The subject of sole proprietors activity with SARs related to personal income withdrawing or transfer to cards:

G - WHOLESALE AND RETAIL TRADE; REPAIR OF MOTOR VEHICLES AND MOTORCYCLES	23.79%
L - TRANSACTIONS WITH REAL ESTATE	15.16%
M - PROFESSIONAL, SCIENTIFIC AND TECHNICAL ACTIVITIES	13.68%
J - INFORMATION AND COMMUNICATION	11.37%
S - ALL OTHER SERVICES	10.53%
F - CONSTRUCTION	7.37%
N - ACTIVITIES IN THE FIELD OF ADMINISTRATIVE AND SUPPORT SERVICES	5.68%
H - ACTIVITIES FOR TRANSPORTATION, WAREHOUSING, POSTAL AND COURIER ACTIVITIES	4.21%
C - MANUFACTURING	4.00%
A - AGRICULTURE, FORESTRY AND FISHERIES	1.47%
R - THE ART, SPORT, ENTERTAINMENT AND LEISURE	1.05%
E - WATER SUPPLY; WASTE COLLECTION, TREATMENT AND DISPOSAL, POLLUTION CONTROL ACTIVITIES	0.84%

The subject of sole proprietors activity (2020 on-boarding):

G - WHOLESALE AND RETAIL TRADE; CAR AND MOTORCYCLE REPAIR	22.79%
H - TRANSPORTATION, WAREHOUSING, POSTAL AND COURIER ACTIVITIES	15.54%
M - PROFESSIONAL, SCIENTIFIC AND TECHNICAL ACTIVITIES	15.52%
J - INFORMATION AND COMMUNICATION	9.24%
F - CONSTRUCTION	8.80%
S - PROVISION OF OTHER SERVICES	8.18%

2018 (before "covid"), it was on-boarded less in twice but activity areas were similar:

G-WHOLESALE AND RETAIL TRADE; REPAIR OF CARS AND MOTORCYCLES	29.56%
S-PROVISION OF OTHER SERVICES	28.81%
H-TRANSPORT, WAREHOUSING, POSTAL AND COURIER ACTIVITIES	14.11%
M - PROFESSIONAL, SCIENTIFIC AND TECHNICAL ACTIVITIES	5.57%
F-CONSTRUCTION	5.11%
J-INFORMATION AND COMMUNICATION	3.52%

- During the verification process, no grounds were identified for further suspension / denial of financial transactions execution.

## 1. The chronology:

2018 - single cases;

2019 - the number of monthly reported cases increased to tens;

2020 - significant increase.

The main target is individuals (vishing / phishing\*).

According to our observations:

- phishing losses occur in 55% of attempts;
- vishing losses occur in 24% of attempts;
- vishing occurs more often than phishing by 50%.

For corporates are more typical (single cases):

- contracts details replacement;
- remote access to the customer's PC.

"Fraudsters" need a withdrawing money channel to complete fraud successfully:

- "fake" persons ("money mule");
- "fair sellers" (further crypto-currencies deals mostly).

\* Phishing - mass mailings are carried out within various services (for example, social networks), sending personal messages (address phishing) to users, which, as a rule, contains a link to a site that looks similar to the original one.

Vishing (English: vishing – voice + phishing) is an oral type of phishing, in which fraudsters, through telephone communication, using techniques, methods and technologies of social engineering, under various pretexts, skillfully playing a certain role (usually a bank employee, a technical specialist, etc.), force a person to tell them their confidential bank or personal data or encourage them to perform certain actions with their bank account or banking card.

## 2. AML methods and measures that were up to date in 2020.

### ✓ EDD for opening accounts, “standard portraits”:

a corporate-resident whose head / founder is a citizen of the Russian Federation (without a residence permit in the Republic of Belarus), whose registration date coincides with the date of opening a bank account (or precedes it for a minor period: a day or two);

an individual: new customer, a citizen of the Republic of Belarus, according to the questioning: unemployed, the main request is non-personalized cards for personal purposes in the maximum as possible number.

### ✓ Suspension / denial of financial transactions execution:

#### Opening an account:

- Transaction’s enhanced control: Compliance’s approval for withdrawals and transfers.

At this stage, a SAR (due to additional behavioral signs), a refusal to open an account, an inclusion into local BL (in order to control further on-boardings) are possible.

## ✓ Suspension / denial of financial transactions execution.

### The account was opened:

- withdraw or transfer attempt;
- suspension (for source of the funds verification) or denial of execution the financial transaction with reference to the AML law;
- SAR sending (depending on the customer's explanations or refusal of explanations – the specified signs in the SAR may differ);
- remote service suspension (it is the possibility provided by the AML legislation), customer notification with reference to the AML law.

Bank can receive the information from third parties about any suspicious transfers or attempts via the bank's Contact Center (**24/7**).

In this case, the reaction will be similar:

- ✓ suspicious customer's account technical blocking immediately;
- ✓ suspension (for source of the funds verification) of execution the suspicious financial transaction (if the money has not yet been withdrawn);
- ✓ denial of financial transactions execution, customer notification with reference to the AML law;
- ✓ remote service suspension, customer notification with reference to the AML law;
- ✓ SAR sending;
- ✓ HRR score and inclusion into local BL (in order to control further business with the customer).

**Thanks for your attention!**