MEETING
OF THE INTERNATIONAL COMPLIANCE COUNCIL
on "Increasing the financial literacy of the clients as a mechanism for reducing the risks of money laundering and terrorism financing"

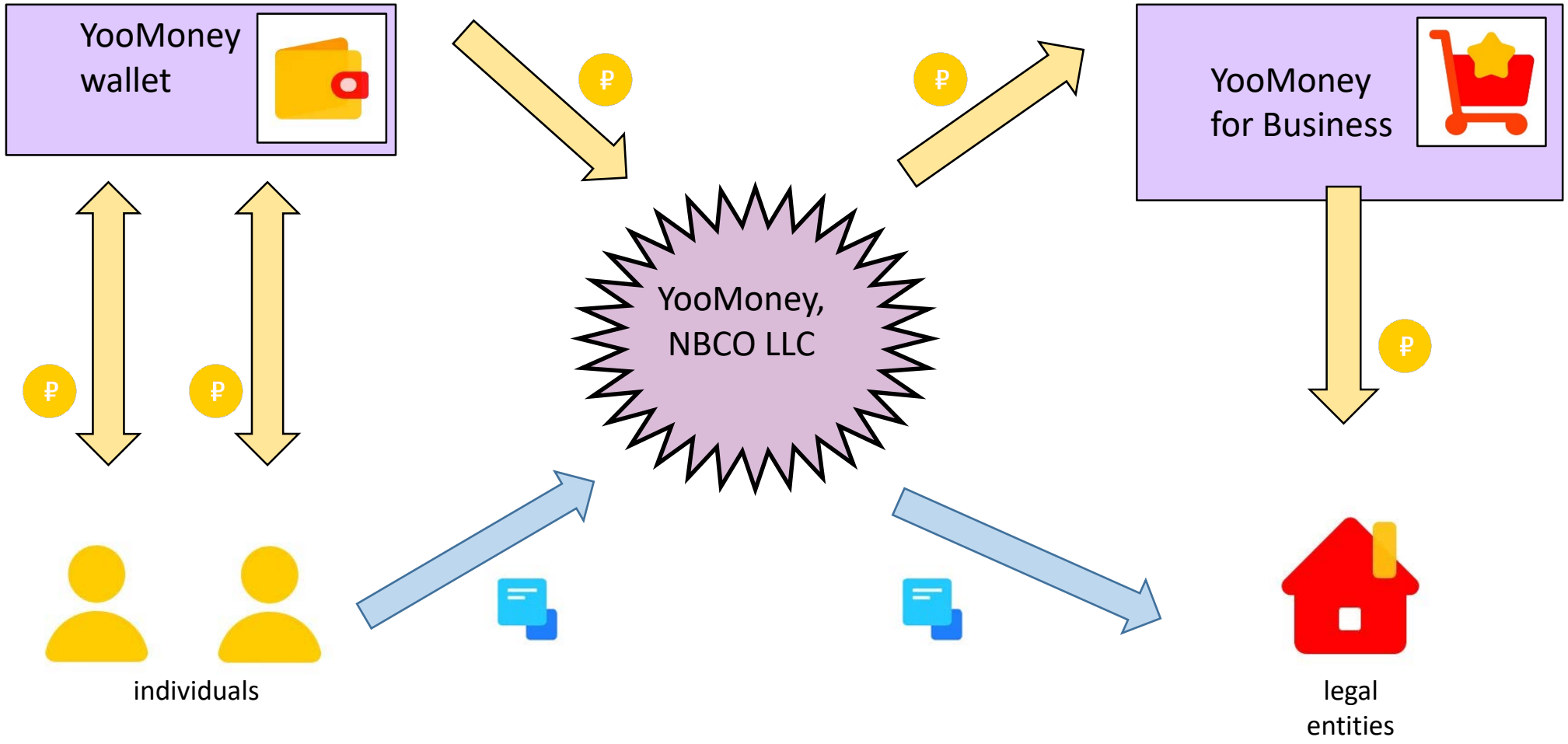
COLLECTION OF PRESENTATIONS

May 25, 2022

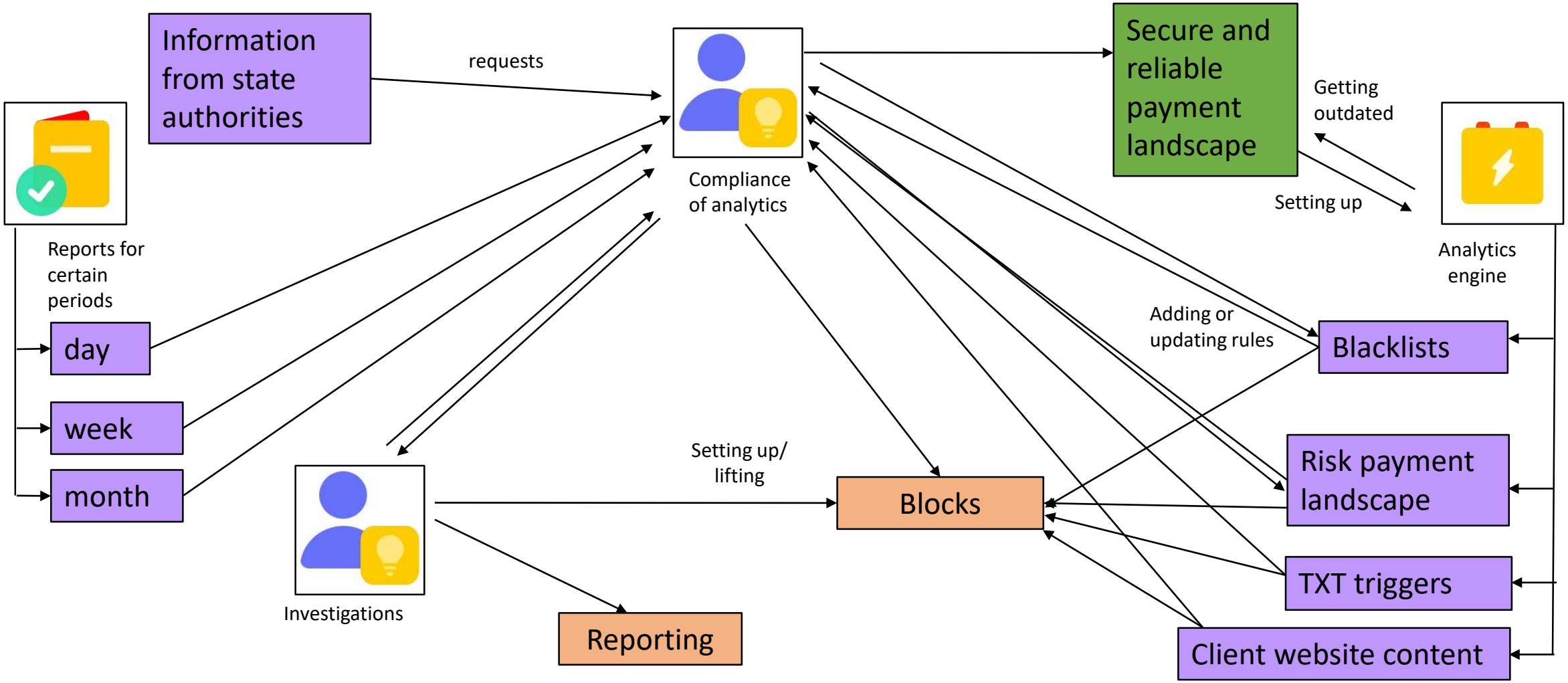
Procedures and automated tools for detecting illegal activity on the financial market (online casinos, crypto exchange, pseudo education online projects, etc.) and reducing risks for customers

Dmitry Gronin,
Head of the Internal Control Department

Our main services



General scheme of monitoring



Monitoring wallets
A prototypical scheme of illegal business activities

Signs of suspicious activity according to methodological recommendations No. **16-MR** from the Bank of Russia dated September 6, 2021**:**

- abundance of transactions and parties;
- the account is almost never idle;
- signs of automated management;
- numerous interactions with other accounts.

Shared account details and things in common:

- devices, cookie
- IDs
- means of payment
- location
- email
- phone numbers
- IP, where money was added from
- …

History of regulatory requirements

- Federal Law No. 355-FZ dated July 2, 2021: responsibility of subjects of AML/CFT to verify licenses
- Federal Law No. 358-FZ dated November 27, 2017: blacklists from the Federal Tax Service regarding casinos and gambling
- Federal Law No. 355-FZ dated July 2, 2021: extraterritoriality of requirements towards casinos
- Federal Law No. 259-FZ dated July 31, 2020: regulation of issue and exchange of crypto currencies
- Federal Law No. 259-FZ dated August 2, 2019: regulation of crowdfunding in the Russian Federation
- Federal Law No. 212-FZ dated July 26, 2017: concept of a nominal account for intermediaries
- Decree of Ministry of Education and Science of the Russian Federation No. 882,
- Decree of Ministry of Education of the Russian Federation No. 391 dated August 5, 2020: regulation of online education

Access points for monitoring businesses

Complaints and feedback

Suspicious account interactions: personalization data, digital footprints, IP, cookie files, phone numbers, e-mail, addresses, login activity, geography of activity, etc.

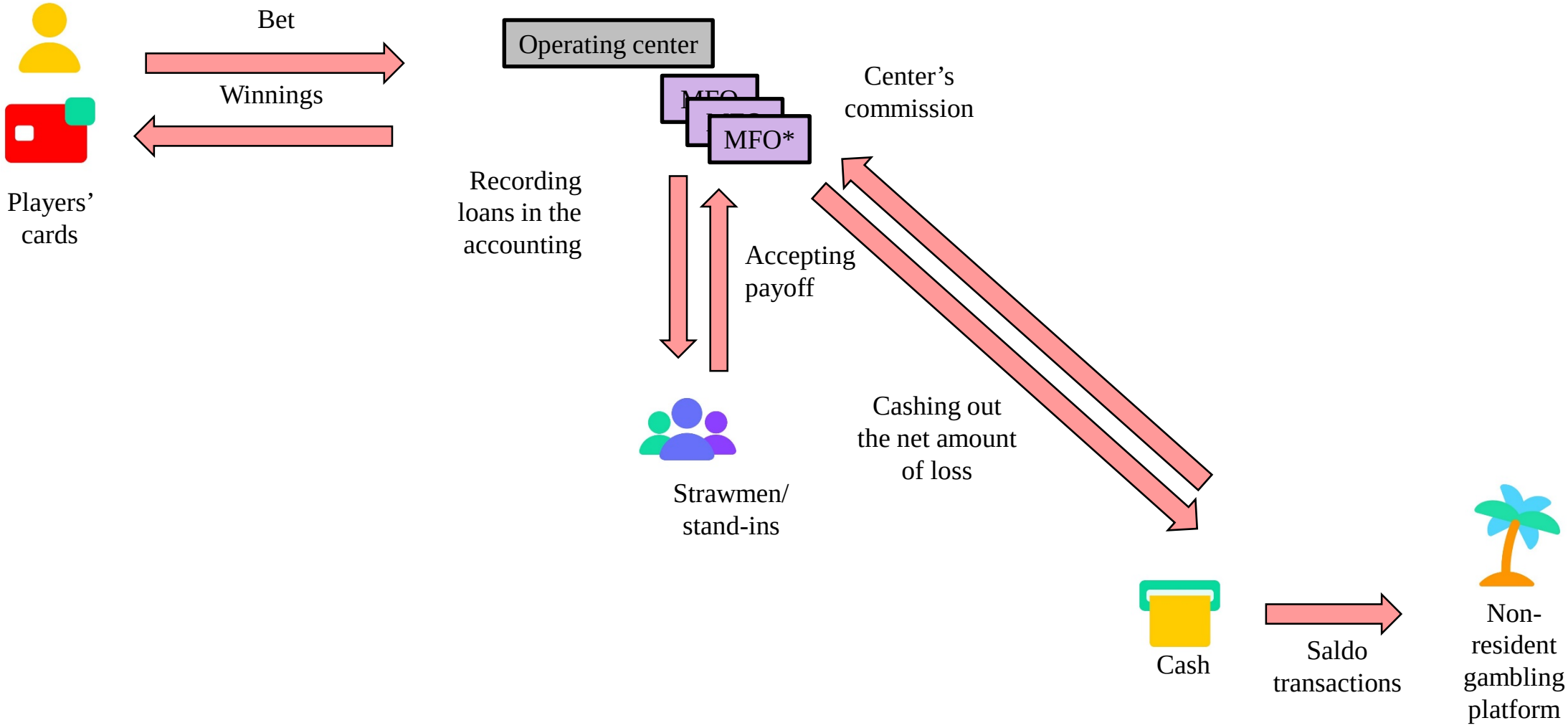
Significant similarities in banking details of payers

Significant editing of website content, key words and phrases appearing

Disparity between the average order value and turnover in the nomenclature of products and services

Other dangerous patterns of payment behavior described with models, payment anomalies regarding amounts, frequency, geography, etc.

Undercover online casinos



* microfinance organizations

Crypto exchange services

Interactions with companies earlier closed or classified as exchange services, judging by various visible factors

There's a big **proportion** of counterparties, whose wallets have earlier been closed and classified as exchange services, in the payment flow

There has been two or more independent **reports** for exchange activity or similar complaints providing an insight into wallet's activity

METHODS OF IDENTIFICATION OF SCAM BROKERS AND PYRAMID SCHEMES

EVERYONE WANTS TO MAKE MONEY

Many people tend to seek ways of earning a lot of money easily and fast.

Quite often, such aspirations make people an easy prey for fraudsters and scammers who run pyramid schemes thoroughly disguised as investment companies, brokers, etc.

It is difficult for an ordinary person to identify fraudsters. In fact, no one is immune to financial scams.

ACCORDING TO THE SURVEY, EVERY TENTH PERSON RESPONDS TO FINANCIAL SCAM ATTEMPTS.

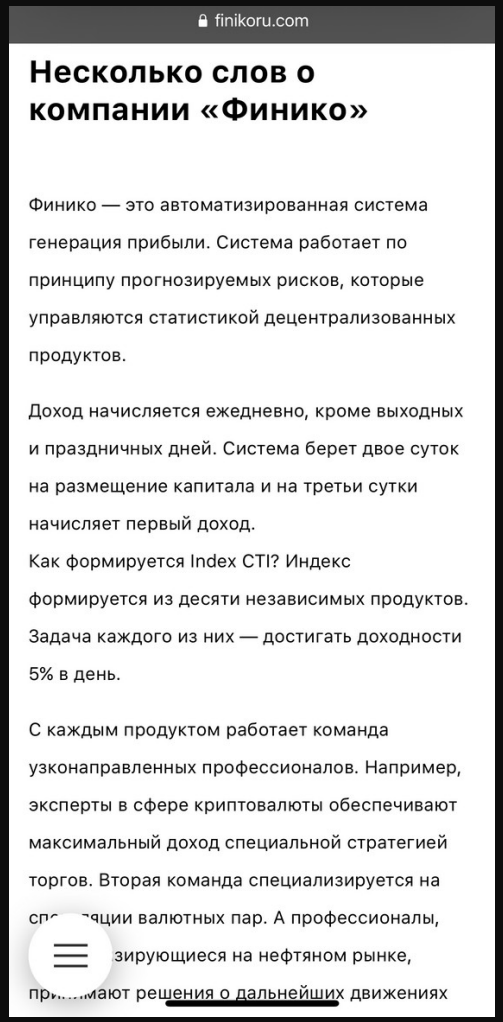
NEW PYRAMID SCHEMES AND COMPANIES (PROJECTS) HAVING “SIGNS OF ILLEGAL ACTIVITY” (I.E. SUSPECTED OF BEING INVOLVED IN ILLEGAL ACTIVITIES) ARE IDENTIFIED EVERY YEAR.

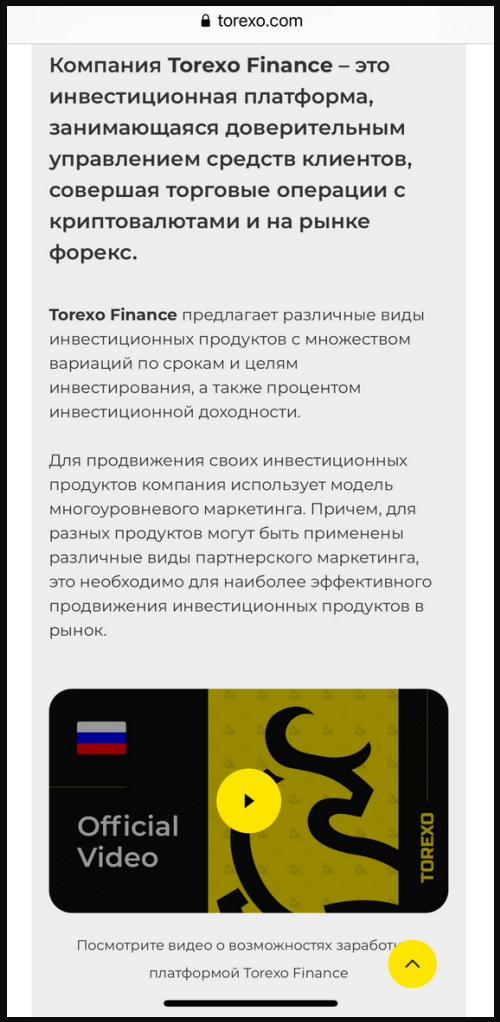
In the Russian Federation, 137 pyramid schemes were identified in 2017; 168 pyramid schemes were identified in 2018; 237 pyramid schemes were identified in 2019; 200 pyramid schemes were identified in 2020; and 146 pyramid schemes were identified in the first half of 2021. Typically, such schemes operate in all CIS member countries.

The Central Bank of the Russian Federation identified 729 companies (projects) suspected of being involved in illegal activities in the financial market in the first half of 2021 alone. The full blacklist of such companies is posted on the official website of the Central Bank of the Russian Federation: www.cbr.ru/inside/warning-list/

2021 TRENDS

The increasing number of pyramid schemes operates through social media and messenger apps. Raising funds from public for investment into various cryptocurrency-related projects was observed as the major trend in 2021. Some pyramid schemes advertise cryptocurrency trust management services, some of them lure people with large revenues from cryptocurrency trading, while others issue their own cryptocurrencies and promise high return of investment into them. However, after a relatively short period when such cryptocurrencies grow in value, their price plunges almost to zero.





WHAT IS A PYRAMID SCHEME?

Pyramid scheme is a fraudulent investment scam in which returns to earlier investors are paid from capital derived from new investors. Pyramid schemes operate in a relatively simple way: operators raise funds from the public promising high return on investments (20-30% per month), and pay profits to earlier investors with funds from more recent investors.

Unlike licensed investment funds or brokers, pyramid schemes are not involved in actual business activities and do not invest funds, but instead they simply collect money from later investors to pay earlier investors.

1. HOW DO PYRAMID SCHEMES CALL THEMSELVES?

Pyramid scheme organizers try to conceal in every possible way the fact that they are almost not involved in any actual business activity. To that end, they operate under the guise of solid financial companies (investment, microfinance, brokerage companies).

For this purpose they invent different names, such as: training course, online earning platform, promising business project, payment service, cashback service, high-tech company, innovative startup, super-efficient production enterprise, etc.

Fraudsters running pyramid schemes offer to acquire stock, bonds, tokens, cryptocurrencies and real estate property, and promise to invest raised funds into highly lucrative production, construction, etc. projects.

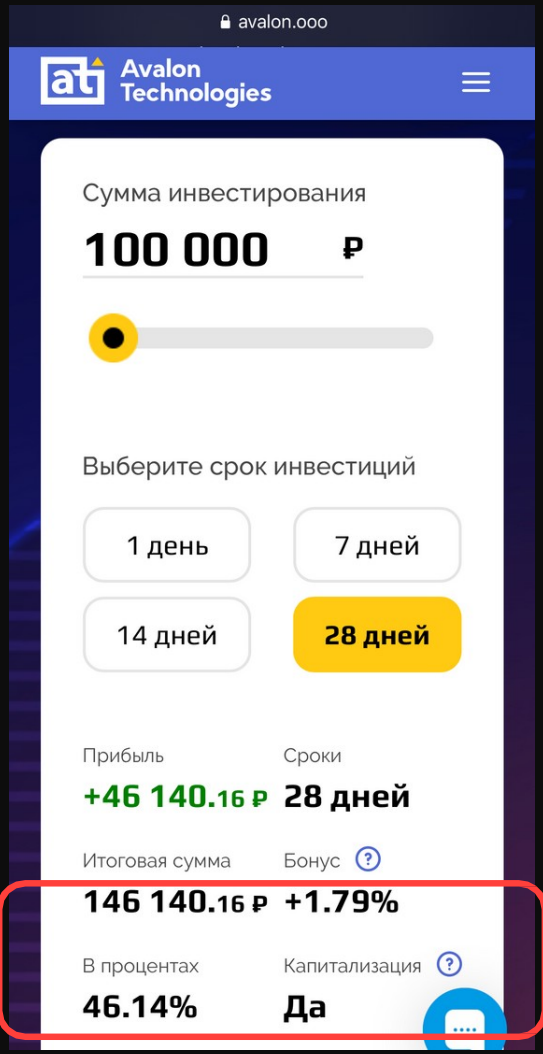
PYRAMID SCHEME INDICATORS

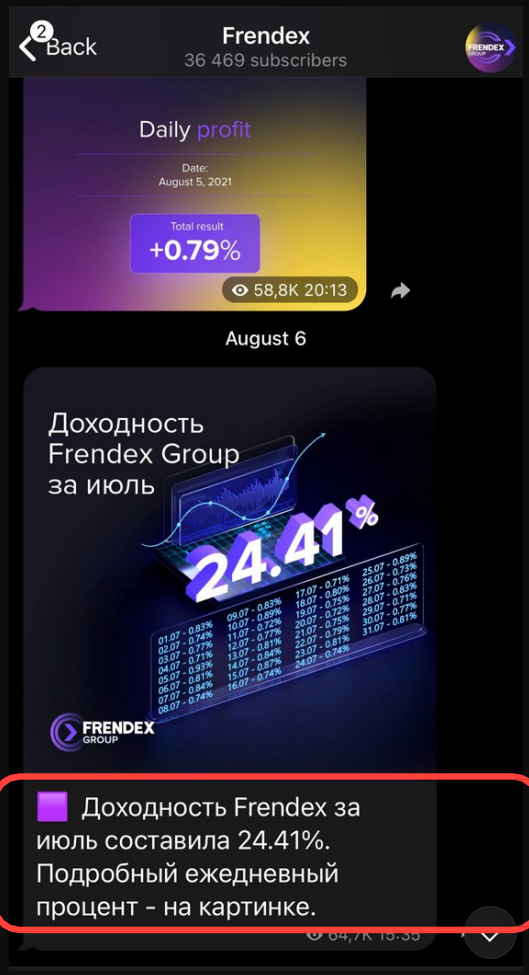
It is very important to know indicators of pyramid schemes, as it will allow you to independently identify such schemes and protect yourself from financial losses.

2. PROMISE OF HIGH RETURN ON INVESTMENTS

Promise of high return on investment is the major indicator of a pyramid scheme. Scammers “guarantee” revenues many times exceeding the market level. In fact, if you are promised revenues in foreign currency (return on your investment) exceeding 1-2% per month, it is highly likely that you are dealing with fraudsters.

Pyramid scheme indicators

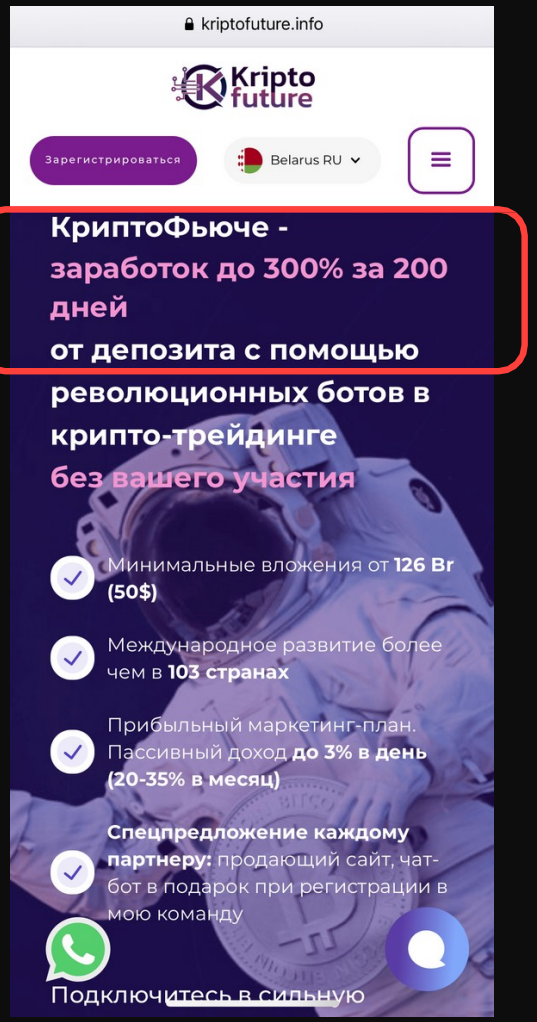


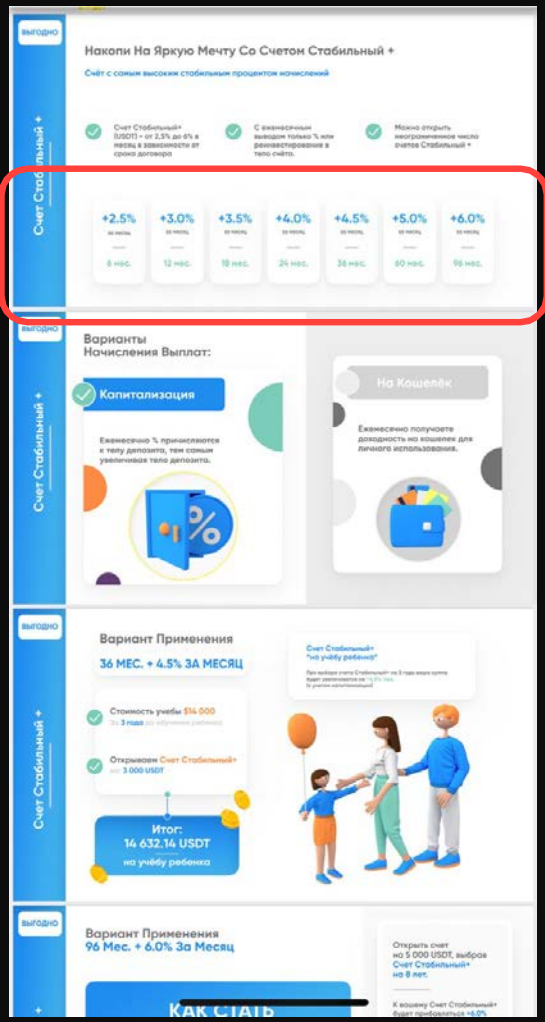


3. GUARANTEED PROFIT

Scammers running pyramid schemes guarantee (promise) future profits and ascertain that there are no risks at all. However, this is not true and never happens in practice, since any investment is associated with risk and, therefore, may lead to financial losses.

Pyramid scheme indicators

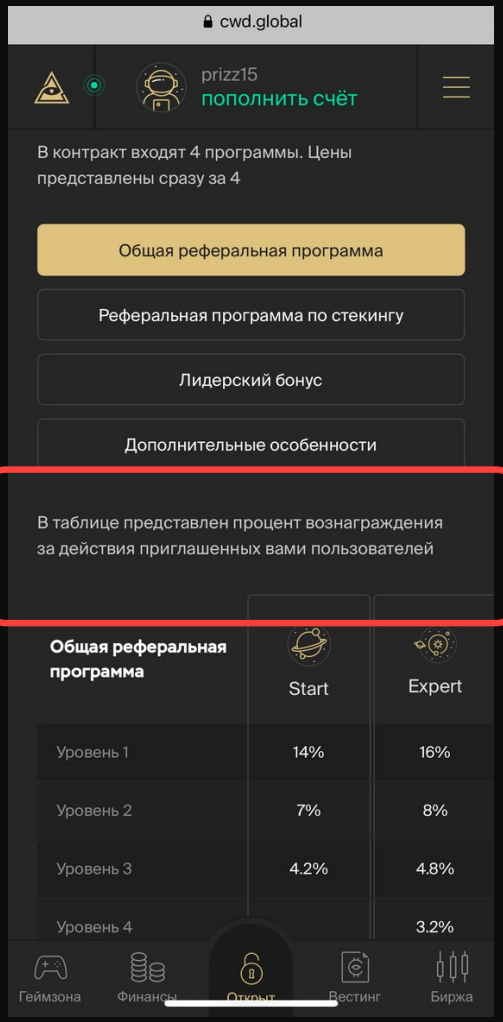




4 Request to Recruit New Clients (Investors)

Use of multi-level marketing (MLM) schemes in the investment sector always raises suspicions. It is pyramid scheme operators that frequently ask (incentivise) clients to bring in new investors from among their acquaintances, paying a percentage of the funds invested by new clients as a commission for each recruited investor. In this way, more and more people get involved in a pyramid scheme.

Pyramid scheme indicators

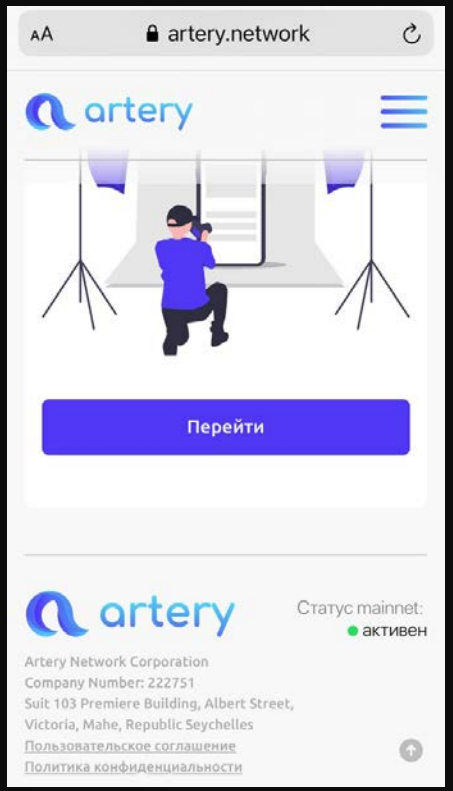


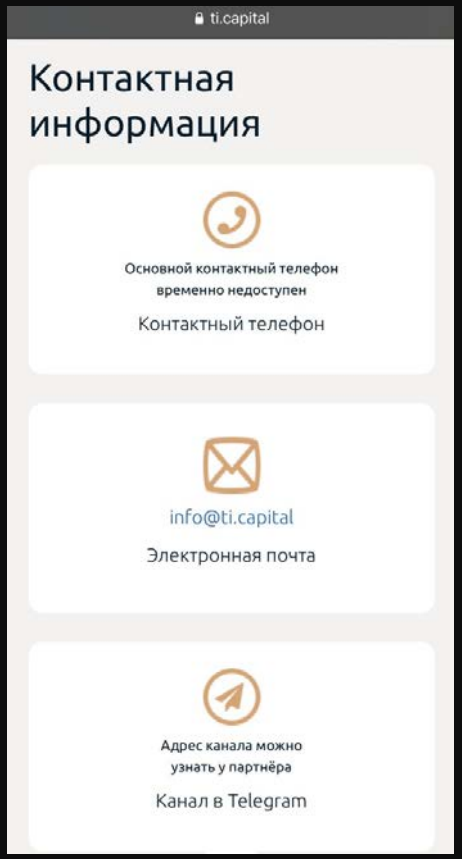
5 ABSENCE OF REAL ADDRESS AND DIRECTOR

No information is available about the physical office of a company, or a company is registered in an offshore zone (British Virgin Islands, Belize, Seychelles, Vanuatu, etc.).

No contact information, including phone numbers and postal address, is provided on a company's website. A website may contain a feedback form and e-mail address at most. Specific information on company's founders and senior managers is also absent. It is only scammers that hide their names and contact details!

Pyramid scheme indicators





6 ABSENCE OF LICENSES ISSUED BY REGULATORS

Absence of a license to carry out investment activities is the strong indicator of a pyramid scheme.

In Belarus, the National Bank operates in the capacity of the regulatory authority.

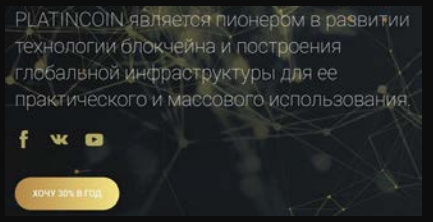
Sometimes, companies may hold licenses to carry out other types of business activities (advisory services, foreign currency exchange) that still do not authorize them to provide investment and trust management services.

Pyramid scheme indicators

7 PROJECT OPERATOR OFFERS TO ACQUIRE ITS OWN CRYPTOCURRENCY

If a company (project) offers to acquire its own cryptocurrency, it is a sound reason for alert. Many projects tried to build their own ecosystems based on the internal cryptocurrency, but the vast majority of them failed. As a result the issued tokens lost their value, and investors ended up with nothing.

Pyramid scheme indicators



8 INVESTMENT THROUGH THIRD PARTIES

If a company asks to transfer money not directly to its account, but through natural persons, it means that you are dealing with fraudsters. Clients are often asked to send money not to the accounts which details are indicated in the contract with the company, but instead to transfer funds to a bank card or mobile phone account of a natural person, or to replenish an e-money wallet or cryptocurrency wallet held by a third party. Sometimes, clients are asked to make payment in cash directly to company’s representatives who issue no deposit receipt or slip in return. As a result, you cannot prove that you have made any payments at all.

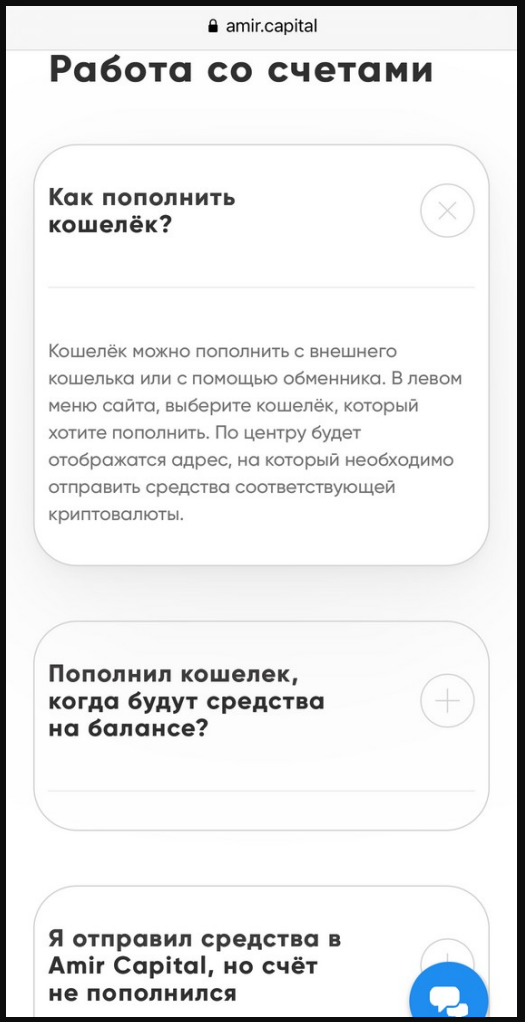
Pyramid scheme indicators

9. Replenishment of Accounts Only by Cryptocurrency

If a company (project) accepts investments from clients only in cryptocurrency, it is a sound reason for alert, since you may be dealing with a pyramid scheme.

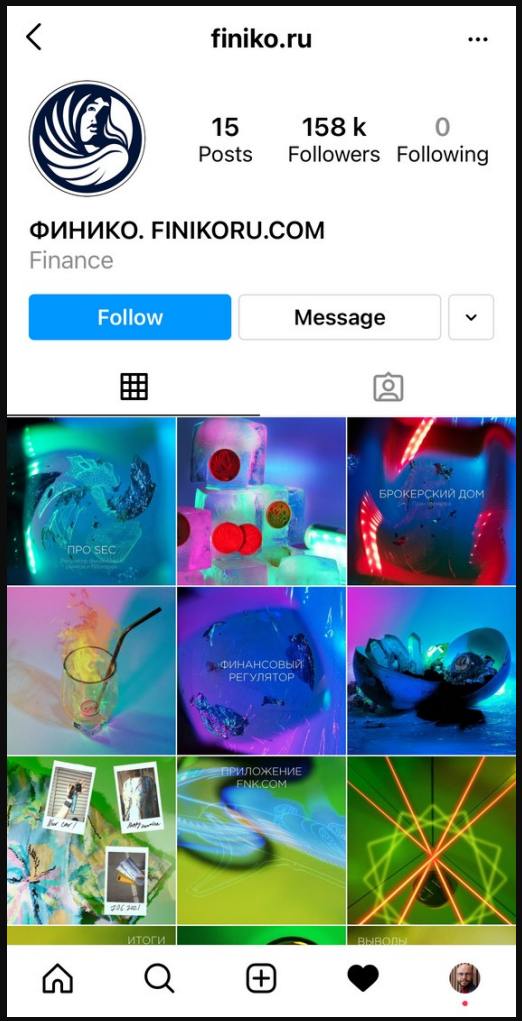
Banks often refuse to open accounts for companies (projects) that are not legally registered in a country or are registered in offshore zones. But even if companies have bank accounts, it does not guarantee that the international payment systems (such as Visa, Mastercard) will agree to transfer funds to the accounts of such companies. Thus, they are not able to receive regular funds and, therefore, are forced to use cryptocurrencies.

Pyramid scheme indicators



10 AGGRESSIVE ADVERTISING CAMPAIGNS

Fraudsters pursue active and aggressive advertising campaigns in social media, messenger apps, presentations, training workshops, etc. For these purposes, they often engage popular bloggers, media celebrities, prominent athletes, etc. who may often be unaware of their misuse by pyramid scheme operators.

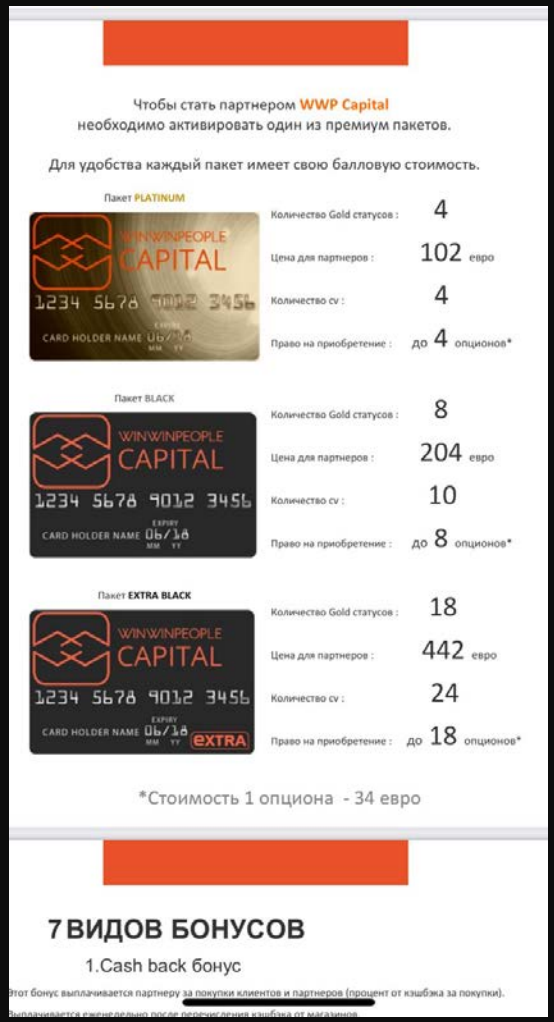


Pyramid scheme indicators

11. CASHBACK SERVICE OFFERS EXPENSIVE PAYABLE SERVICE PACKAGES

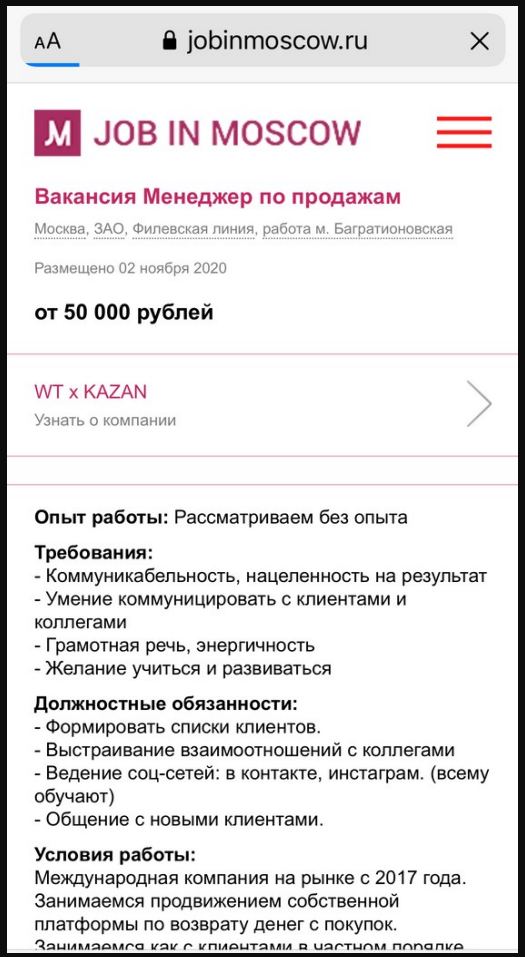
Most cashback services are completely legitimate businesses. But, if representatives of such services persuade clients to acquire expensive VIP, Premium or other service package (card), it is a sound reason for alert. Typically, such service packages oblige clients to seek and bring in new users of this service, as in case of multi-level marketing schemes.

Pyramid scheme indicators



12 REQUEST TO INVEST MONEY DURING EMPLOYMENT

Quite often, pyramid schemes are masquerading as reputable companies that look for administrators, managers, executive officers, consultants, etc. Candidates to these positions are invited to undergo training, after which they should make a payment for some product, service, account activation, membership, etc.



Pyramid scheme indicators

HOW NOT TO BECOME A VICTIM OF PYRAMID SCHEME?

Before investing your money into a company, you should thoroughly check this company.

13. CHECK IF A COMPANY HAS A PROPER LICENSE

Companies should be licensed by the regulator to raise investors' funds and provide trust management services. It is the guarantee that the government authority oversees the operation of a company.

However, if a company shows the license issued by an offshore jurisdiction, this should alert you. Such licenses may be forged or borrowed. You may check on the websites of the regulators whether or not a company holds a proper license.

How not to become a victim of pyramid scheme?

National Bank (Belarus)
https://www.nbrb.by/finsector/forex/register

Central Bank of Russia
https://www.cbr.ru/fmp_check/

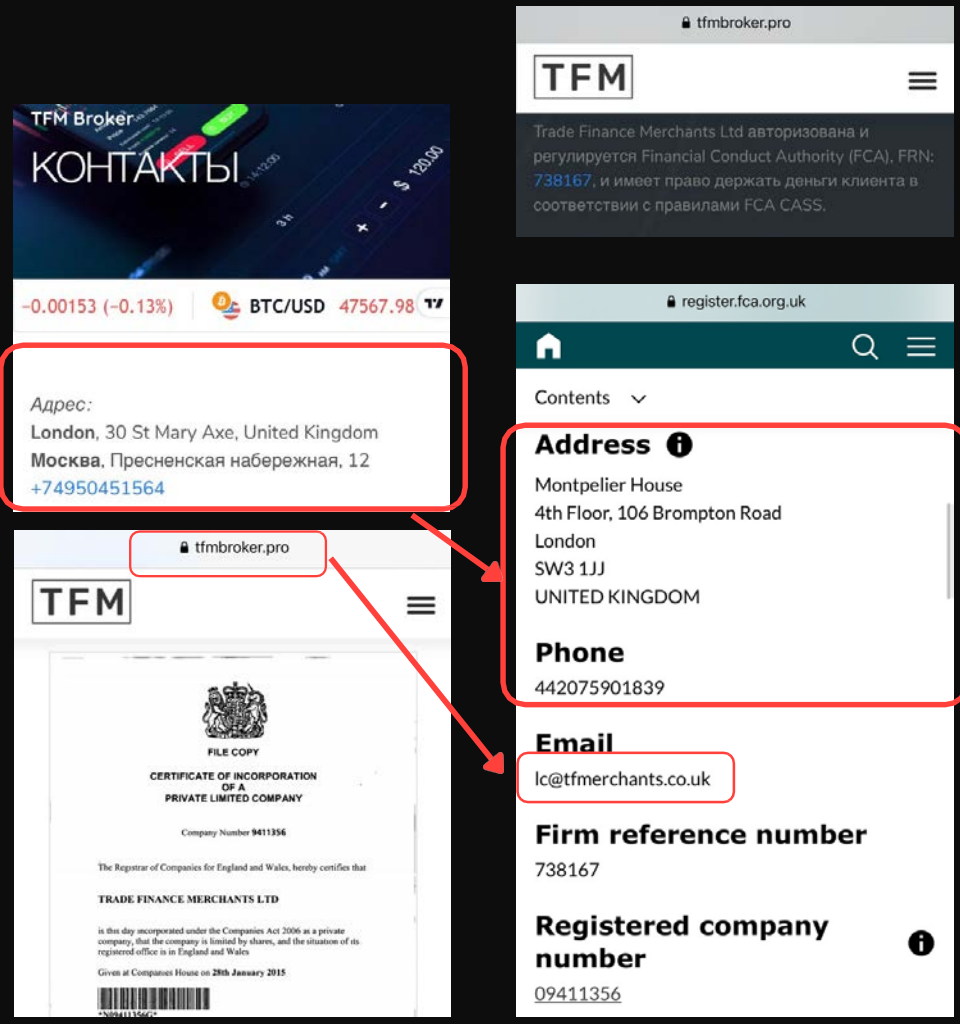
CySEC (Cyprus)
https://www.cysec.gov.cy/en-GB/home/

FCA (UK)
https://register.fca.org.uk/s/

14. EXAMINE COMPANY'S DOCUMENTS

If a company shows its license, cross-check the name and details of the company indicated in the contract and on its website with the information contained in the registers of the regulators. Even small discrepancies may indicate that someone tries to deceive you. Examine, what obligations are undertaken by the company, and what will happen if it fails to fulfill them. It is possible that, already at this stage, you will understand that the company is not worth dealing with.

How not to become a victim of pyramid scheme?



HOW TO IDENTIFY WEBSITE OF A PYRAMID SCHEME?

Quite often, mere examination of the website of a company (project) is enough to understand that it is the pyramid scheme.

15. VERIFY THAT POSTED PHOTO PICTURES ARE THE ORIGINALS

Verify that the photo pictures posted on the website are the originals. For this purpose, you need to save a photo picture posted on the company's (project) website, and after that, upload it into Yandex and Google image search engines. If the photo picture is not the original and has been repeatedly used on other websites, it is highly likely that you are dealing with the pyramid scheme. Financial fraudsters and pyramid scheme operators quite often use stolen photo pictures.

Yandex image search engine
https://yandex.ru/images/

Google image search engine
https://www.google.ru/imphp

How to identify website of a pyramid scheme?

16 CHECK DOMAIN REGISTRATION DATE

Date of domain name registration, i.e. domain age, can be checked on website: who.is. Since scammers have to change websites quite frequently, the age of their domains is typically less than ONE year.

Domain Checker Service
https://who.is/

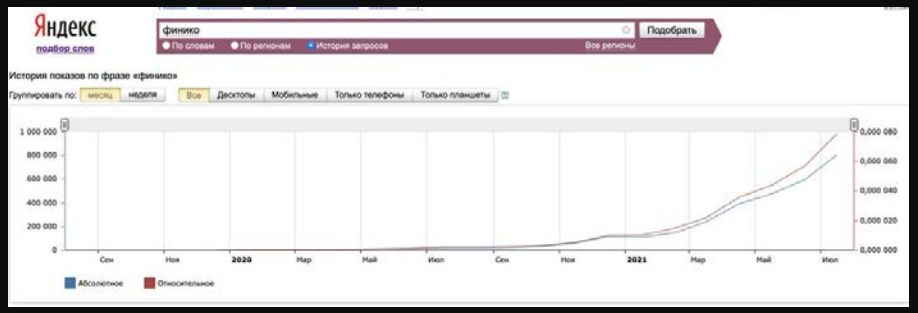
Pyramid scheme operators often publish misleading information about length of time they operate in the financial markets.

How to identify website of a pyramid scheme?

17. CHECK TIME PERIOD OF OPERATION OF A COMPANY

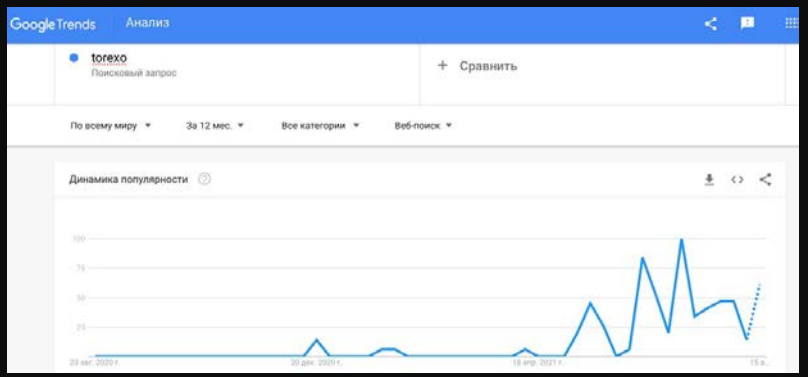
History of users' search queries involving a company's brand name in Yandex Search will show the real time of operation of the financial company.

https://wordstat.yandex.ru/



If such search queries have appeared only recently, while the company states that it has a long experience, this should alert you. If a company positions itself as the international one, it is better to use Google Trends for analyzing search queries involving its name.

https://trends.google.ru/trends/



How to identify website of a pyramid scheme?

18 Check Phone Numbers

Pyramid scheme operators often call clients using local phone numbers, while in reality they stay abroad. For this purpose, they use IP telephony. Existence of negative reviews about the project can be verified by way of examining people’s reviews about phone numbers used by fraudsters to make calls on the following websites: zvonili.com and neberitrubku.ru.

Search for reviews by phone number
https://zvonili.com

Search by phone number
https://www.neberitrubku.ru

How to identify website of a pyramid scheme?

19 Check Reviews for Integrity

Pyramid scheme operators actively use Yandex and Google search engine result pages to “flood” the first pages with fake positive reviews about their work, so that true and honest reviews appear on the bottom pages and are not read by users. For this purpose, they use bots, create fake websites, purchase positive reviews, etc.

The experience shows that satisfied clients rarely provide feedback on financial services, since they consider such services confidential. If you see a lot of positive reviews, this should alert you and may indicate that you are dealing with fraudsters.

How to identify website of a pyramid scheme?

Reviews on the following websites are considered more trustworthy:

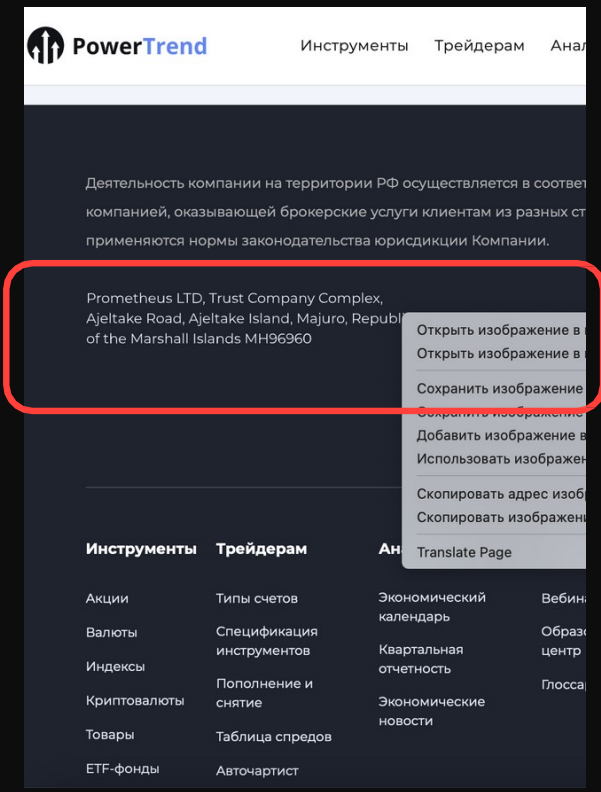
Network-Trust
https://trustorg.com

Reviews on Google Maps
https://www.google.com/maps

Reviews on Yandex Maps
https://yandex.by/maps

20 CHECK WEBSITE INDEXING

If a portion of textual information posted on a project website cannot be copied (as an image), it is highly likely that such a website is owned by fraudsters. They do it intentionally so that their websites are not indexed by search engines. Information about legal entity is often displayed in such manner.



How to identify website of a pyramid scheme?

ORIENBANK

Presentation in the frame of the international compliance council meeting

Improving the financial literacy of clients as a mechanism risks mitigation of money laundering and financing of terrosim

General definition of financial literacy

Financial literacy is a sufficient level of knowledge and skills that allows you to make informed and effective decisions in various areas of personal finance management, such as savings, investments, real estate, insurance, tax and retirement planning.

Why is it important to improve financial literacy?

The lack of financial literacy of a significant part of the population limits the ability of people to effectively manage their funds, make the right decisions about their financial future, and thus force them to take high financial risks. This creates positive environment for the reproduction of structures involved in money laundering, financing of terrorism and using the population for these purposes.

Why is it important to improve financial literacy?

The ever-increasing number of financial products, their complication, the displacement of responsibility for individual financial decisions from the state and financial institutions to individuals increase the need to improve the financial literacy of clients of financial institutions.

Why is it important to improve financial literacy?

- Financial illiteracy acts as a "catalyst" for the increasing the risk of an individual being involved in money laundering schemes.
- A risk-averse financially illiterate person may be involved in illegal financial transactions as a victim, a "blind instrument" of defrauders.
- A risk-averse financially illiterate individual is exposed to an even greater risk of this kind, since he may be involved as an executor in money laundering schemes.

Why is it important to improve financial literacy?

FINANCIALLY LITERAL PERSON:

- Keeps records of income and expenses;
- Has savings;
- Knows his rights;
- Spends less than earns;
- Has up-to-date financial information;
- Knows how to choose financial services.

Why is it important to improve financial literacy?

Financial literacy allows the decision maker to identify proposals associated with the potential risk of financial fraud and, accordingly, refuse to participate in them.

This extends to individuals with varying financial risk appetites, with the exception of highly risk averse individuals (commonly referred to as “gambling persons”), for whom participation in money laundering activities may have their own usefulness.

Methods used by banks to improve the financial literacy of customers

1. Training of employees
2. Training of clients
3. Simplify product descriptions
4. Making contracts easier to understand
5. Customer advice in branches
6. Placement of informational articles on the website

Methods used by banks to improve the financial literacy of customers

Distribution of printed information materials

Tasks that can be solved by financial literacy of clients

• 1. Promotes the activation of the population participation in operations in the financial market, the formation of rational financial behavior and the use of a wider range of financial products and services.

• 2. Helps maintain financial stability and contributes to combating money laundering and financing of terrorism by increasing market financial discipline within the frame of financial system

Tasks that can be solved by financial literacy of clients

3. Supports the stability of financial institutions and expands their ability to accumulate sufficient funds to finance the real sector of the economy, the needs of businesses and households.

4. Contributes to the formation of literate consumers of financial products and services who perceive the financial system in a comprehensive manner and understand the values of financial institutions.

The need to take into account the level of financial literacy of clients when managing risks of ML/FT

- Modernization of modern risk management tools in the field of money laundering or terrorist financing is impossible without taking into account the level of financial literacy of clients of financial institutions.

- It is important to understand that a client's actual level of financial literacy does not correlate with their propensity to take on increased risks.

- At the same time, a low level of financial literacy and a high risk appetite increase the risks of financial institutions and form a new risk zone in the field of money laundering or financing of terrorism.

Recommendations for risks studies in the field of ML/FT depending on the level of financial literacy of clients

- The study of risks in the field of AML/FT, depending on the level of financial literacy of clients, should be carried out based on the development of risk classification according to key features:

— by clients or clients categories;

— by types of financial transactions.

- This will allow financial institutions to identify and apply appropriate control measures and mechanism to reduce them.

Risk STUDY recommendations

Identify Risks

Assess risks

Understand risks

Risk analysis

Recommendation for risk analysis

- Risk analysis should always be carried out at the very beginning of forming a relationship with a client - based on a complete analysis of the information provided by him.

- The level of financial literacy of a client can only be determined after the client has made several transactions through a financial institution based on monitoring these transactions and regularly updating risk assessments.

- In this case, the risk management of financial institutions in the field of money laundering or financing of terrorism is implemented through a system of tools - established by regulators and developed by financial institutions themselves, taking into account the financial literacy of clients.

COMPONENTS

- FOLLOWING SLIDES WILL PRESENT THE COMPONENTS OF THE RISK MANAGEMENT SYSTEM OF FINANCIAL INSTITUTIONS IN THE FIELD OF ANTI-MONEY LAUNDERING OR FINANCING OF TERRORISM WITH CONSIDERING FINANCIAL LITERACY OF CLIENTS.

Risks in the field of ML/FT

1. Country/geographic region risk
2. Client risk
3. Product (service) risk

Prerequisites for the risks formation in the field of ML/FT

1. Applying to a financial institution for one-time transactions

2. Unclear economic meaning of the operation

3. Critical amounts (significantly above or below of prudential standards)

4. Intensive customer transactions with cash

Risk management tools

1. Clients identification

2. Development by a financial institution of criteria and signs of suspicious transactions

3. Extended control over operations by customer categories

4. Formation of unreliable clients database in respect of which suspicious transactions were identified

Risk management tools

5. Accumulation of information in a financial institution about customers and financial transactions

6. Implementation of training programs for employees and clients of financial institutions

Monitoring procedures with the purpose to mitigate risks in the field of ML/FT

1. Documentary verification of clients

2. Identification of transactions that fall under the criteria for transactions subject to mandatory control

3. Assessment of the level of financial literacy of clients based on the history of their service in a financial institution

4. Control over the well-timed improvement of the professional knowledge level in the field of AML/FT by employees of financial institutions

CONCLUSION

- **The risk management system of financial institutions in the field of money laundering or financing of terrorism is essential for ensuring the stability of the functioning of financial institutions, is dynamic and complex in content.**

- **This makes it possible to identify the vector for modernizing the risk management tools of financial institutions in the field of combating money laundering or financing of terrorism based on improving the financial literacy of their individual clients.**

Thank you for your attention!

Ак Барс Банк

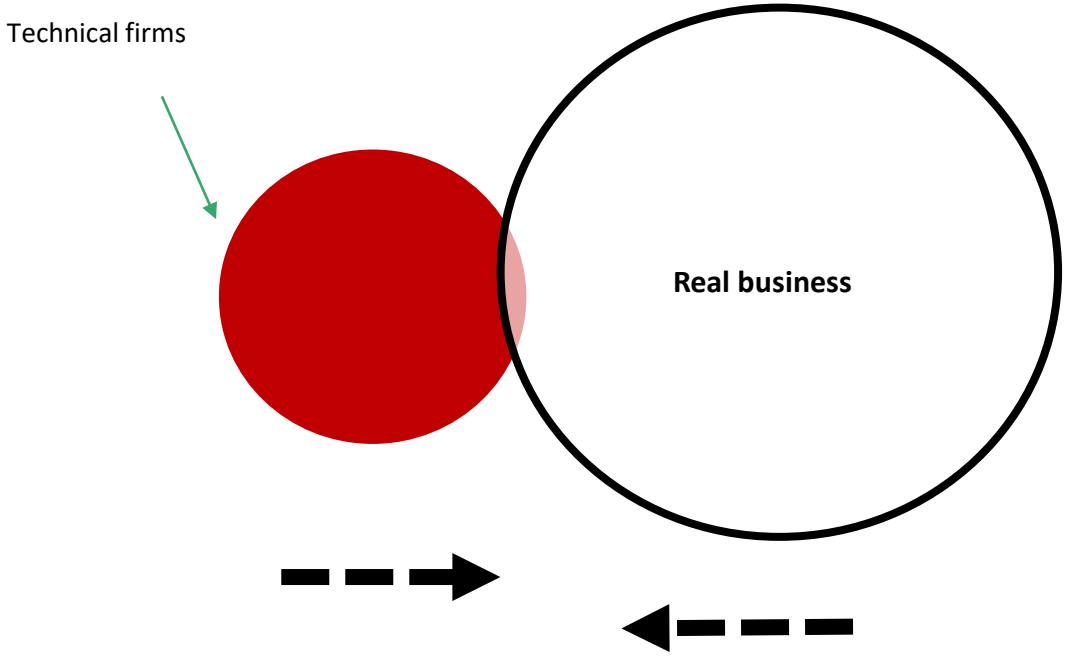
Improving financial literacy of clients as a tool to reduce AML risks

International Compliance Council
May 25, 2022

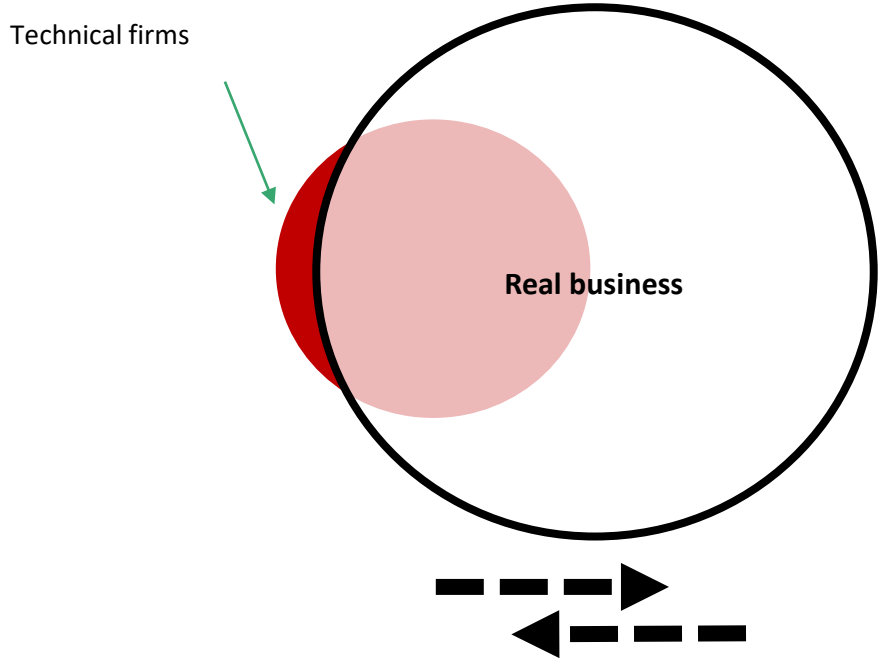
Speaker: A.R. Bagaviyev
Head of Compliance

Increasingly, real business (bona fide clients) become(s) participant(s) of shadow schemes

As it used to be:



What it is now:



*At the same time, the number of empty shell companies in Russia has **decreased by 10 times** since 2016 (from 32% to 3.1%)*

Why the client falls under risk area

The desire to receive "easy money" without predicting the consequences

Impulsivity in making decisions without proper analysis of the situation

High willingness to take risks. Neglecting the responsibility

Ignorance of the regulatory environment.
Ignorance / disregard of the measures of responsibility

The lack of opportunity to obtain the necessary expert advice (economists, lawyers, etc.)

Ак Барс Банк

Common schemes for conducting illegal transactions involving persons with low financial literacy

Often, clients show sincere surprise and indignation of inquiries from credit institutions, despite the fact that in some cases they are engaged in direct money laundering

- Cashing in in the guise of paying wages
- "Fan-like" cashing in various manifestations
- Sale of cash trade receipt
- Cashing in using corporate cards
- VAT breaking

- Participation in the mass opening of cards / drop card
- Becoming a nominee director/founder in a technical firm
- Use of electronic / virtual wallets
- Withdrawal of funds through cryptocurrency

Such schemes are identified and counteracted by credit institutions in coordination with Rosfinmonitoring

Ак Барс Банк

Compliance tools development trend

What it is now:

- *Investigations*
- *Bans*
- *Limits*
- *Refusals*
- *Documents query*
- *Relations termination*
- *Fee increase*
- *Control Control Control Control Control ...*

What else shall be added:

- *Training*
- *Attitude development*
- *Culture*
- *Awareness*
- *Warning*

The possibility of involving trustworthy market participants in illegal activities largely depends on the level of financial literacy of the latter. **This parameter can be increased by the efforts of banks**

Improving financial literacy through education / training of clients is one of the important tasks of credit institutions

Ак Барс Банк

Developing a culture of compliance in the Bank

"Complicated Things in a Simple Way"

The effectiveness of the compliance system is based on each employee's personal responsibility, from senior management to an ordinary employee of the bank. Development of clients' financial literacy starts from the formation of rules, way of thinking and raising awareness of each employee of the Bank

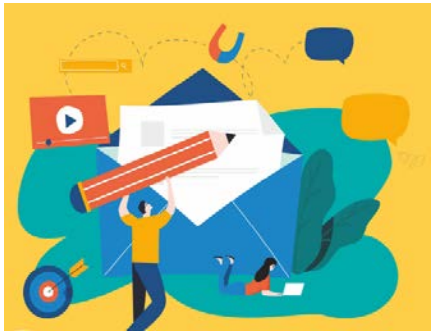
Tools for developing a culture of compliance:

Awareness-raising campaigns:

- A compliance series and topic-based posters have been created
- Publications in the corporate news newspaper
- Annual anonymous survey on corporate ethics and collection of employee suggestions for improving the process
- Compliance Champion Competition with souvenir prizes

Training:

- Online multimedia courses
- Full-time training
- Communication with the manager and key employees, including receiving feedback
- Training meetings with partners of the Bank
- Mentoring and increasing new employees' involvement



Development of the communication channel:

- A compliance hotline has been created
- The Compliance Department staff are open for communication with employees on any compliance issues

Transparency of processes:

- Program for developing a culture of compliance has been approved
- Processes aimed at compliance with norms and rules are transparent and clear to employees, recommendations on building effective relationships with customers are given

Ак Барс Банк

Projects on improving AK BARS BANK clients' financial literacy

Training communications cover more than 200 thousand people

Round tables, meetings with businesses (8 meetings in 2021)

University students' participation in educational programs (for Law and Economics Faculties)

Participation in the International Financial Security Olympiad

Revizor Service (risk assessment by 24 parameters)

Publication of articles in the media

Educational material on television

Play-based training for children

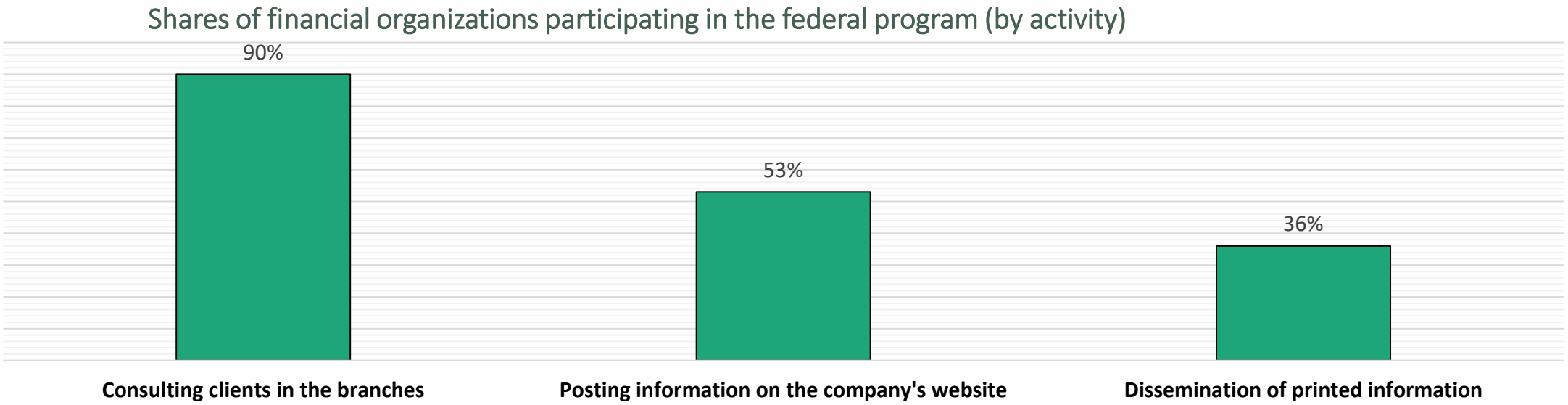
Memory cards, manuals for clients (when opening an account, during bank servicing)

Materials are in the application, on the Bank's website: courses, tests, articles.

Ак Барс Банк

The Bank participates in preparation of educational programs for students, holds events and round tables for entrepreneurs, prepares information materials for the media. Our projects reach a broad audience – from children to pensioners

“Online Financial Literacy Lessons” Federal Program



Online financial literacy lessons have been held since 2017. They contribute to the formation of principles of responsible and competent approach to financial decision-making among the rising generation. Specialists of Russia's leading financial institutions conduct educational webinars for schoolchildren from more than 1.5 thousand schools across the country. 14 organizations and their regional representative offices from among professional participants of the securities market, banks, insurance companies, universities, government bodies participate in the project as partners. **In 2018, AK BARS Bank joined the federal project.**

Ак Барс Банк

Ак Барс Банк

Thank you for your attention!

Regulation of Digital Asset Service Providers (DASP) in the AIFC

AFSA Astana Financial Services Authority

Contents

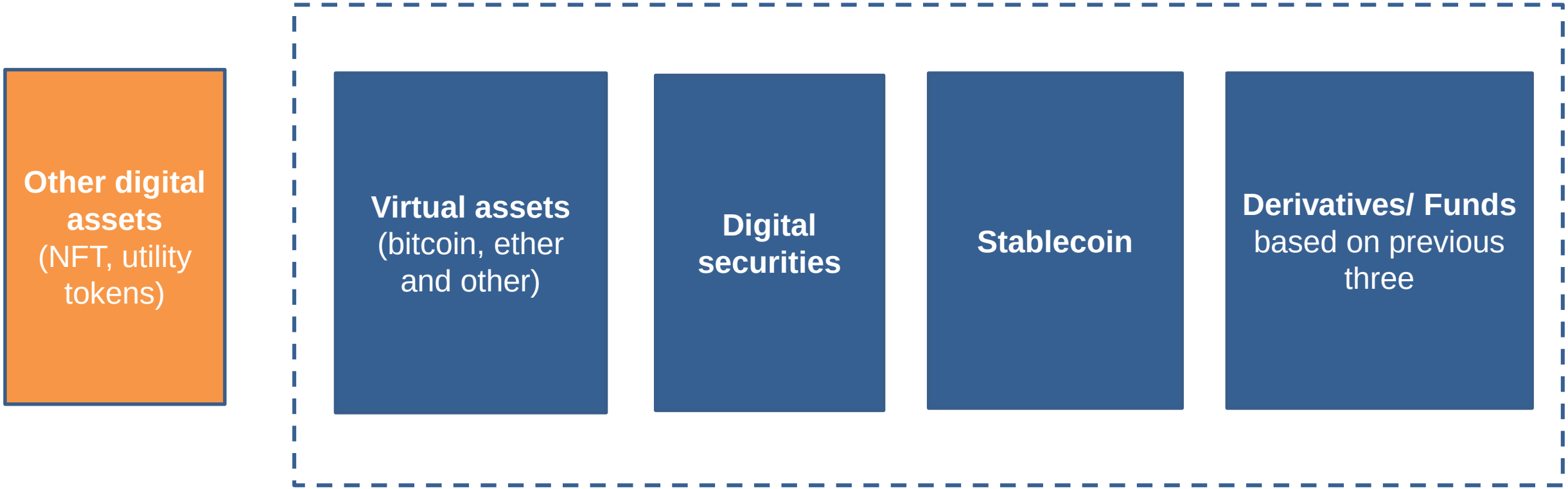
1. The current situation in the world
2. Perimeter of DASP regulation in AIFC
3. AIFC Legal regulation of DASPs for AML/CFT
4. Features of the Supervision and Control over the VASPs in the AIFC for AML/CFT
5. Regulatory sandbox regime

AFSA Astana Financial Services Authority

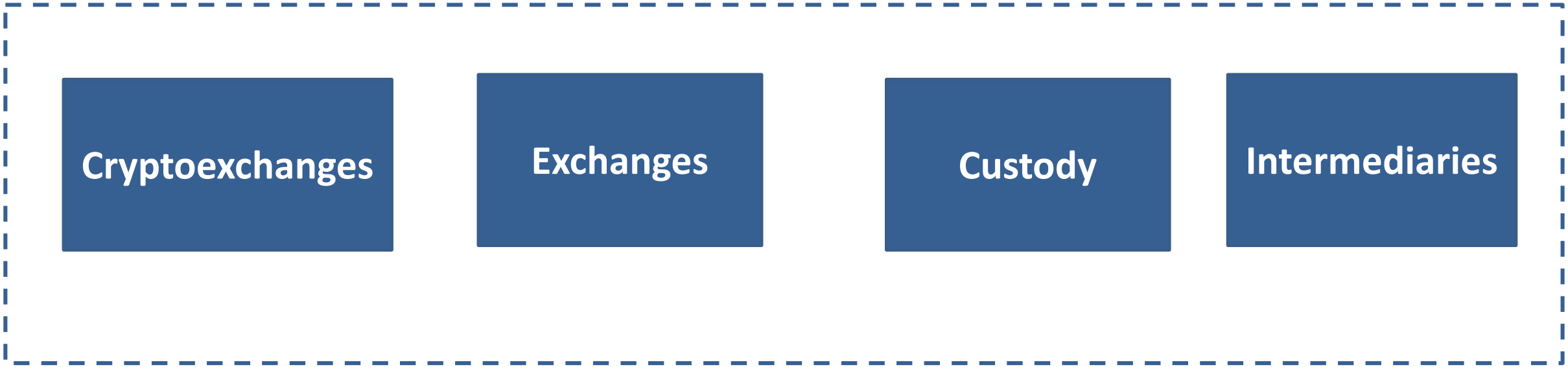
The current situation in the world

- The global cryptocurrency market reached a value of US$ 1,8 billion in 2021. Looking forward, the market is projected to reach US$ 32,4 billion by 2027 (Yahoo Finance).
- According to report of «Chainalysis», total transaction volume grew to $15.8 trillion in 2021, up 567% from 2020 totals.
- Despite this, the company's report on the use of digital assets for criminal purposes noted that the share of the use of digital assets for such purposes was only 0.15% of the total turnover of digital assets in the world.

Perimeter of DASP regulation in the AIFC



DASPs in AIFC



Key normative legal acts and rules regulating DASPs activities in the AIFC for AML/CFT

- Kazakhstan's AML/CFT law
- AIFC AML Rules
- AIFC Financial Technology Rules
- AIFC Financial Services Framework Regulation
- AIFC Companies Rules
- AIFC General Rules
- AIFC Business of Conduct Rules
- AIFC Prudential Rules
- AIFC Market Rules
- AIFC AMI Rules
- **…**
- **There are more than 80 legal acts and rules in total regulating DASPs activities in the AIFC for AML/CFT**

Key requirements for DASPs

- Systems and Controls for AML/CFT.
- Application of a Risk-Based Approach to business and client assessment.
- AML/CFT/PWMD risks assessment.
- Application of enhanced CDD measures with regard to VASP clients.
- Assessment of risks associated with electronic transactions, new technologies, products and channels for information sharing and providing services.
- Identification and reporting to the FIU on the suspicious and threshold transactions.
- Undertake client monitoring and CDD on the UN/FATF/Kazakhstani Sanctions Lists.
- Ensure MLRO training (at least once in a year).
- **…**
- **The requirements have been developed in compliance with the Kazakhstan's anti-money laundering (AML) and counter terrorist financing (CTF) law and FATF Recommendations**

Key criteria and requirements for DASP authorisation (licensing) in the AIFC

Risks Control

- ❑ Get registered with the FIU's data collection and processing system to report on STR/TTR.
- ❑ Comply with the STR/TTR reporting requirements.
- ❑ Development and Testing Plans of the product/service
- ❑ Policies and Procedures:
  - AML/CFT
  - Risk-management (incl. operational, IT, legal, fraud, business continuty)
  - Compliance
  - Business conduct
  - IT
- ❑ Client agreement that outlines the risk disclosure measures required by the VASP's license.
- ❑ Comply with the AIFC material outsourcing requirements.
- ❑ DVASP must ensure that Client Money is held in a segregated Client Money Account with a third-party account provider that is a Bank or a Regulated Financial Institution.
- ❑ Systems and Controls to prevent conflict of interest and insider trading.
- ❑ DASP must have arrangements in place to ensure storage of Client funds on a Hot Digital wallet.

Operational Resources

- ❑ Financial and nonfinancial resources, including:
  - The availability of adequate funds to meet at least 12 months of operational expenses.
  - Approved/designated individuals:
    - ✓ SEO
    - ✓ Finance Officer
    - ✓ Compliance Officer
    - ✓ Internal Auditor
    - ✓ Money Laundering Reporting Officer (experience and qualifications are important)
    - ✓ Risk Officer
- ❑ The software and other necessary technical equipment.

Regulatory sandbox regime

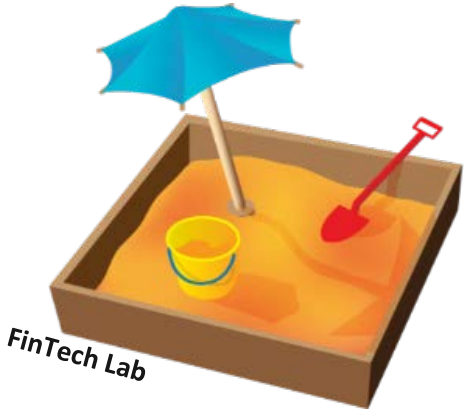
Limits:

- Overall: 5,200,000 USD
- Retail clients: 200,000 USD
- Accredited: 5,000,000 USD

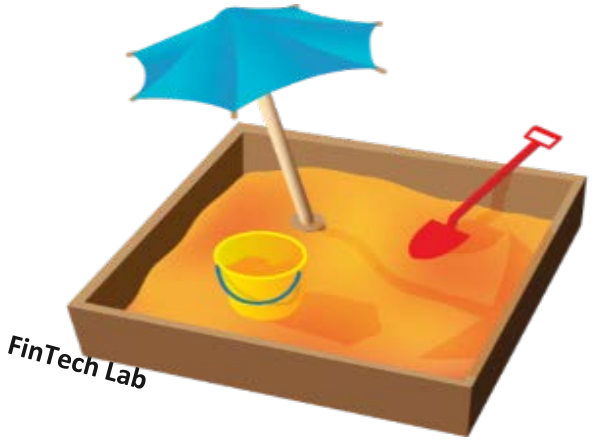
- Retail Client does not invest an amount which exceeds the greater of (over a period of one month):

- USD 1,000; or

- the lesser of (i) 10 percent of the annual income; or (ii) 5 percent of the net worth of such Retail Client, up to a maximum aggregate amount of USD100,000.



Regulatory sandbox regime



- ❑ No Fiat money
- ❑ No P2P transactions
- ❑ No anonymous transactions

Thank you!

AFSA Astana Financial Services Authority

QuantDART

Activities of cryptocurrency brokerage companies as AIFC participants in the fields of AML/CFT

Cryptocurrency regulation in Kazakhstan

Kazakhstan legislation

Digital assets are a type of **asset**

Secured
by real assets

✓ **Turnover is allowed**

Unsecured
e.g. BTC, ETH, DOGE

✗ **Turnover is prohibited**

AIFC

Digital assets are a type of **investment**

Activities regulated by the AIFC :

Crypto exchanges

Crypto brokers

Crypto custodians

Main legal acts of AIFC regulating activities in the field of digital assets

- AIFC framework provisions on financial services
- AIFC General Regulations
- AIFC Rules of Conduct for the Business of AIFC
- AIFC Financial Technology Rules
- AIFC authorized market organisation rules (for crypto exchanges)
- AIFC Anti-Money Laundering, Counter-Terrorist Financing and Sanctions Regulations (AML Regulations)
- Guidelines (requirements) for AML/CFT internal control regulations for financial monitoring entities of AIFC
- Guidelines (requirements) for AML/CFT purposes applicable to customer due diligence when an AIFC Participant establishes a remote form of customer relationship
- List of financial services and related services provided by AIFC participants, subject to financial monitoring
- AIFC prudential rules for investment firms

About QuantDART

Crypto-brokerage:

Buy / sell / exchange digital assets

Trust management:

- 5 investment products
- Min. amount to invest from 100 USD

Custodial services:

Opportunity to obtain a cryptocurrency security guarantee

Link to the public register:

https://publicreg.myafsa.com/details/191240900083/

The official status of this licence can be verified at www.afsa.kz

AIFC | AFSA

LICENCE FOR CARRYING ON REGULATED ACTIVITIES

This is to certify that

Quantdart Fintech Limited

(Business Identification Number: 191240900083)

is an

AUTHORISED FIRM

in accordance with the Acting Law of the Astana International Financial Centre (AIFC). It is authorised subject to compliance with the requirements, conditions, restrictions and/or directions of the Acting Law of the AIFC and requirements set out in the documents attached (if any) to conduct the following Regulated Activites:

1) Dealing in Investments as Principal; 2) Dealing in Investments as Agent; 3) Managing Investments; 4) Advising on Investments; 5) Arranging Deals in Investments - Permitted Investment type: Asset backed tokens; 6) Providing Custody - Safeguarding and administering Asset backed tokens belonging to another Person

This Licence is granted by the Astana Financial Services Authority, the independent regulator of the AIFC

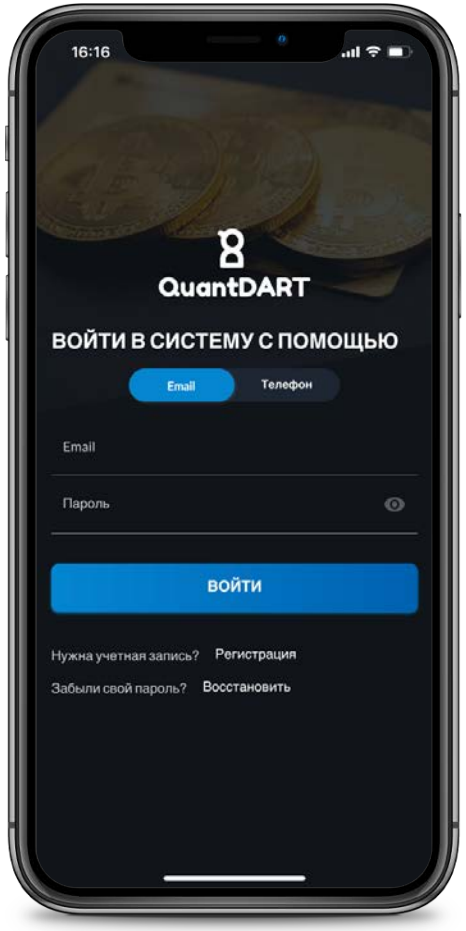
Nurkhat Kushimov
Registrar of Companies
Astana Financial Services Authority

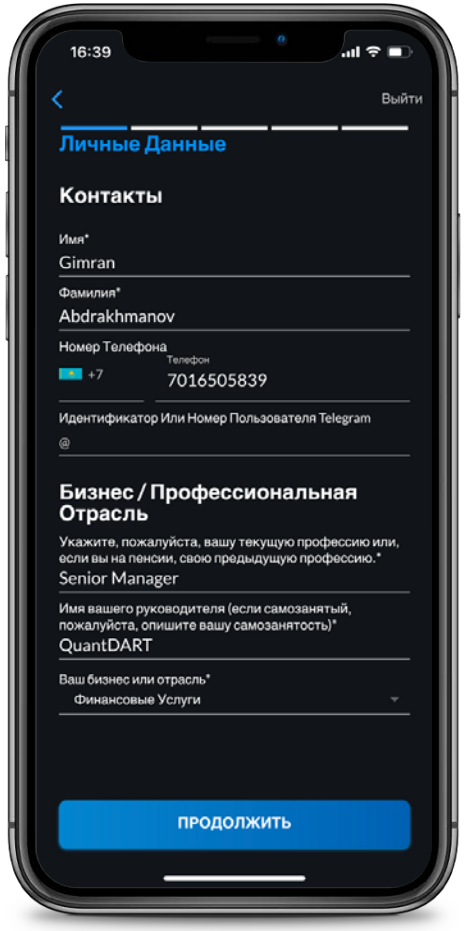
Issue Date: 23 November 2021 Expiry Date: 17 December 2022 Licence Number: AFSA-G-LA-2020-0012

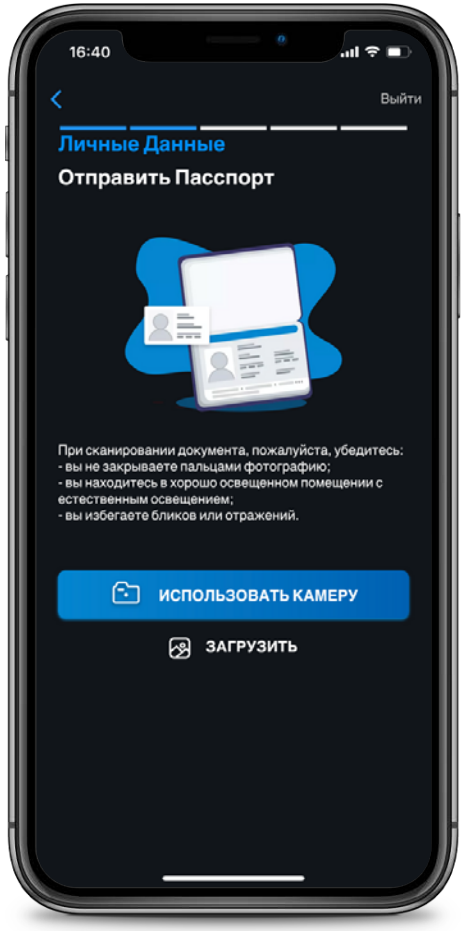
Types of customers

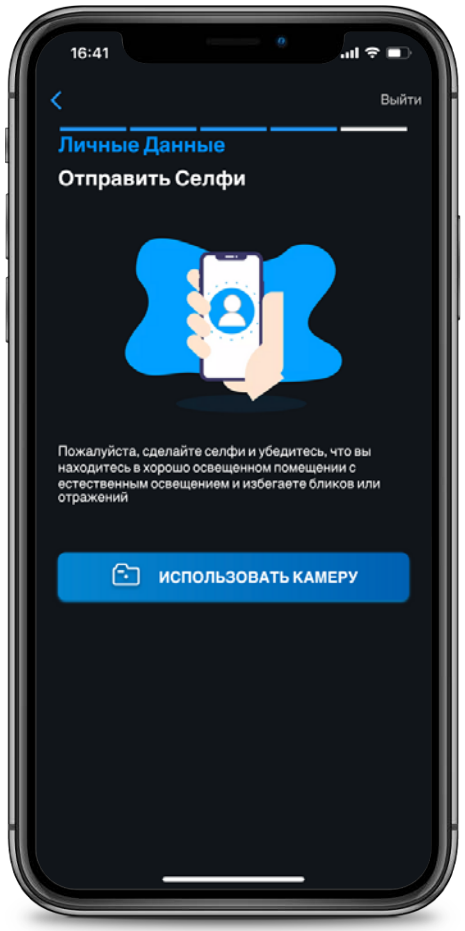
Individuals	Legal entities
Retail client • Deposits of up to 1 BTC or equivalent are permitted • Investments from the equivalent of 100 USD	**Retail client** • Deposits of up to 3 BTC or equivalent are permitted
Professional client • Net assets of at least 100 000 USD • At least 2 years' experience with similar financial products or services	**Professional client** • Net assets of at least 1 000 000 USD • Sufficient experience and understanding of relevant financial products and services

Registration process

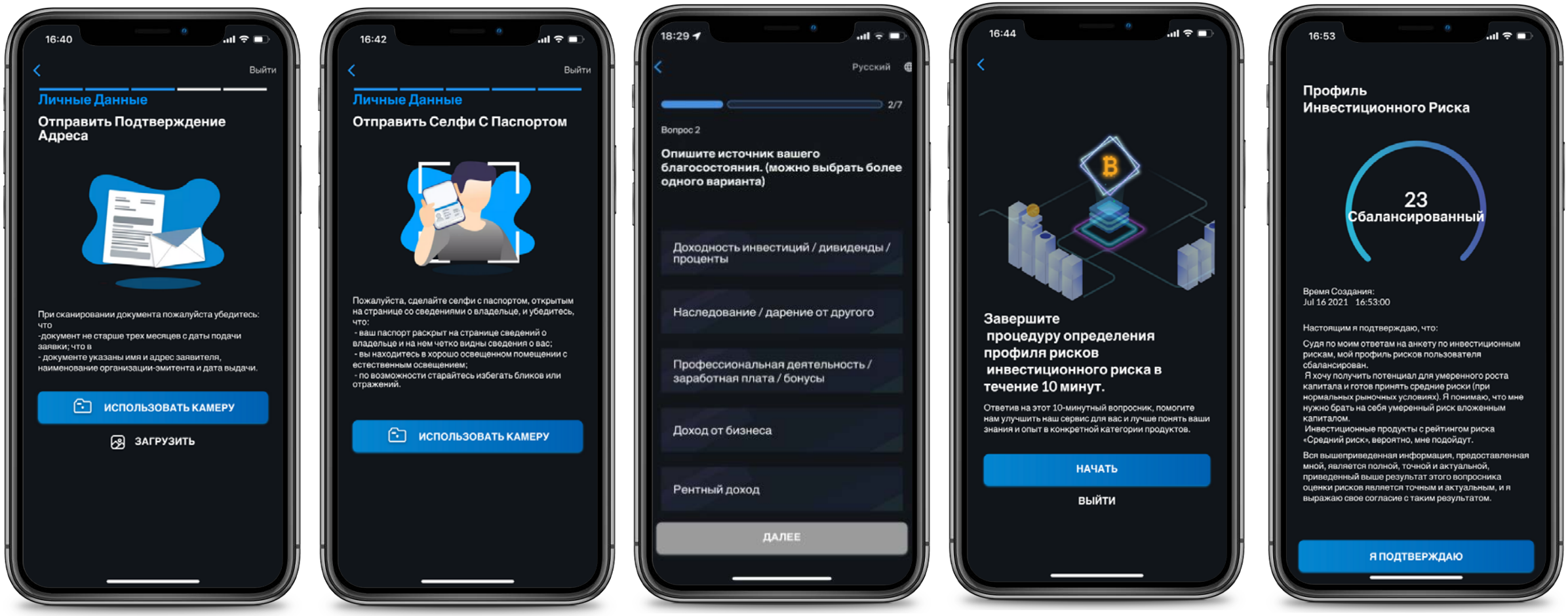








Registration process



General requirements for crypto brokers

AML/CFT policies and procedures established
Accountability to the regulator (AFSA) and FAU

Immediate reporting to the regulator of any breach or likely breach of rules by the company

Minimum capital requirements
Provision of a bank **guarantee** or **insurance**

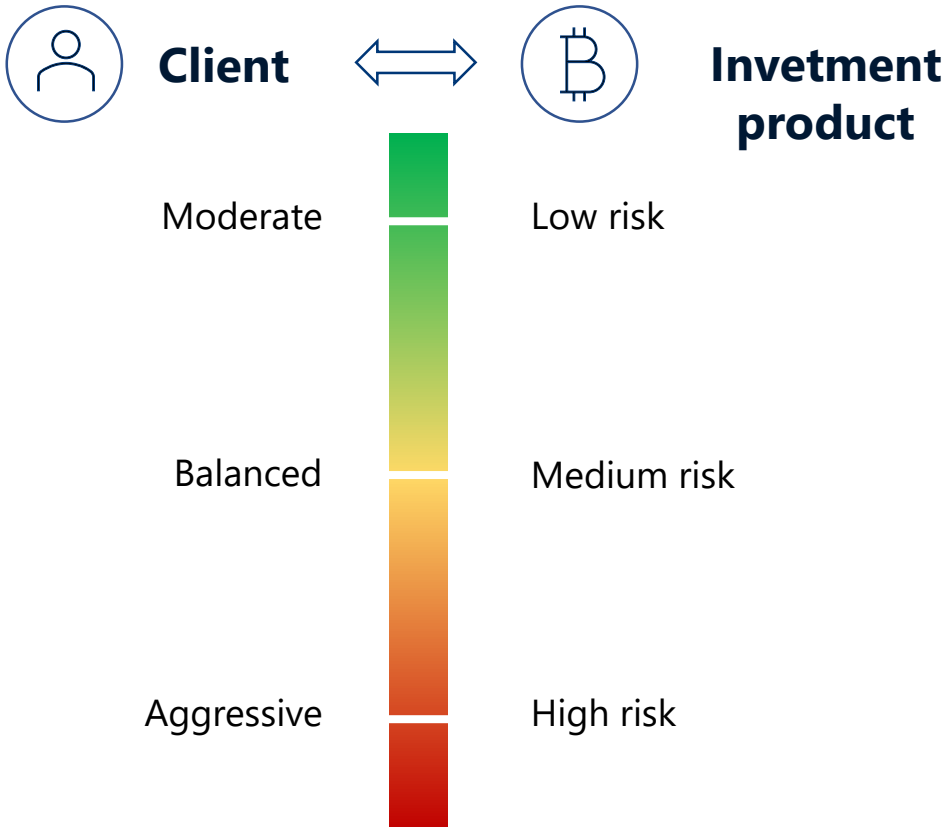
Ensuring 100% **backup** of private keys in a **cold wallet**

IT system requirements
Personal data **protection standards**

Financial audit and **IT audits** by a certified information security auditor

Customer protection

Matching product risk to customer appetite



Separating client fiat money and client digital assets

- Client money or investment accounts are never mixed with company money or digital assets
- Regular reporting to clients

Client agreement

- Regulatory status of the company
- Name and address of beneficiary company (if any)
- Disclosure of all fees and charges

AML/CFT programmes

1) ML/TF program - provides for the organization of an ML/TF system by responsible persons within the company.

2) ML/TF risk management program - risk assessment, risk identification, and mitigation

3) Client Identification Program - AML Policy by AIFC requirements and RK Legislation

4) Transaction monitoring and review program – scrutinize transactions thoroughly and regularly, compare with client risk profiles, and identify anomalies.

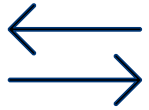
5) Training and education program - regular professional development in line with amendments and changes to standards and legislation.

AML/CFT procedures

Know your customer

- Confirmation of identity
- Understanding / confirming the source of wealth
- Determination of AML/CFT risk rating

Know your transactions



- Accept customer money only from the customer's bank account
- Checking cryptocurrency transactions

Know your supplier

- Verification prior to the establishment of the business relationship
- Continuous monitoring of the relationship

Know your employees

- Enhanced checks on key positions
- Annual reviews

AML/CFT procedures

Responsible persons and monitoring

- Money Laundering Reporting Officer and Compliance Officer - appointed by the Board of Directors and report regularly to the Board of Directors
- Appointment of deputy MLRO (Money Laundering Reporting Officer Deputy)
- Conducting a regular (annual) AML/CFT audit (internal/external) which should take into account
  - random testing for compliance with customer due diligence procedures
  - a review of all notifications sent to the person in charge to identify deficiencies in procedures
  - reviewing the nature and frequency of dialogue between senior management and MLROs
- Annual enterprise-wide AML/CFT risk assessment: product, service, channel risks

AML/CFT procedures

Responsible parties and monitoring

- Training for all staff, including Board of Directors members (annually and when legislation changes)
- Testing of knowledge at the end of the training
- Training and professional development of responsible persons in NGO "Association of Financiers of Kazakhstan" continuously
- Courses, seminars, and trainings organized by UN and OSCE
- Certificate of successful testing at the “National Center for Civil Service Personnel Management” JSC
- Training on the investigation of cryptocurrency transactions

Risk-based approach

- Customer risks
  - Determination of the customer's AML/CFT risk, which will determine the extent of customer due diligence (SDD, CDD, EDD)Determination of the level of ongoing monitoring applied to the business relationship.
- Geographical risks
  - FATF blacklists/grey lists, sanctioned jurisdictions, tax havens/offshore
- Product and service risks
  - Anonymity of digital assets, the novelty of financial instruments and products
- Risks in transactions
  - Threshold and suspicious transactions (TTRs, STRs)
- Risks in delivery mechanisms, channels, and partners
  - Remote establishment of business relationships: biometric customer identification, address verification
  - Abandonment of simplified customer verification

PEPs and beneficial owners

- The following due diligence measures apply to PEPs:
  - obtaining approval from management to establish a business relationship
  - taking reasonable steps to establish the source of the customer's wealth and source of funds
  - Applying enhanced monitoring of the business relationship.
- Beneficial owners ≥ 10% ownership interest in legal entities

Threshold and suspicious transactions

- Threshold and suspicious transactions are reported to the Agency through the WEB-SFM system, followed by notification to the Committee
- Inputs and outputs of digital assets are checked through the database of the blockchain analytics tool
- Threshold transactions are defined in accordance with internal policies and messages are sent no later **than one business day** following the day of the transaction
- Suspicious transaction reports are sent before the transaction takes place or if transactions are not deemed suspicious **before the transaction** takes place, **no later than 24 hours** after the transaction is deemed suspicious
- Immediate freezing of funds of persons and entities subject to sanctions and resolutions, issued by the UN Security Council of the Republic of Kazakhstan, and persons on the list of entities and individuals involved in terrorist financing
- Suspend transactions if the activity, account, or customer transactions are investigated by the MLRO
- Not informing the person (tipping off)

QuantDART

Tracking cryptocurrency transactions: Blockchain Intelligence Group

Blockchain Intelligence Group, headquartered in Vancouver, Canada, has developed a blockchain search engine with data processing and big data analytics.
BIG is a leading developer and provider of cryptocurrency risk assessment and data analysis tools, training and investigation services.

Some of the organizations we've trained

BANK OF AMERICA

DEPARTMENT OF JUSTICE FEDERAL BUREAU OF INVESTIGATION

U.S. DEPARTMENT OF HOMELAND SECURITY

UNITED STATES SECRET SERVICE

WELLS FARGO

Deloitte.

SYGNUM

HSBC

JPMorganChase

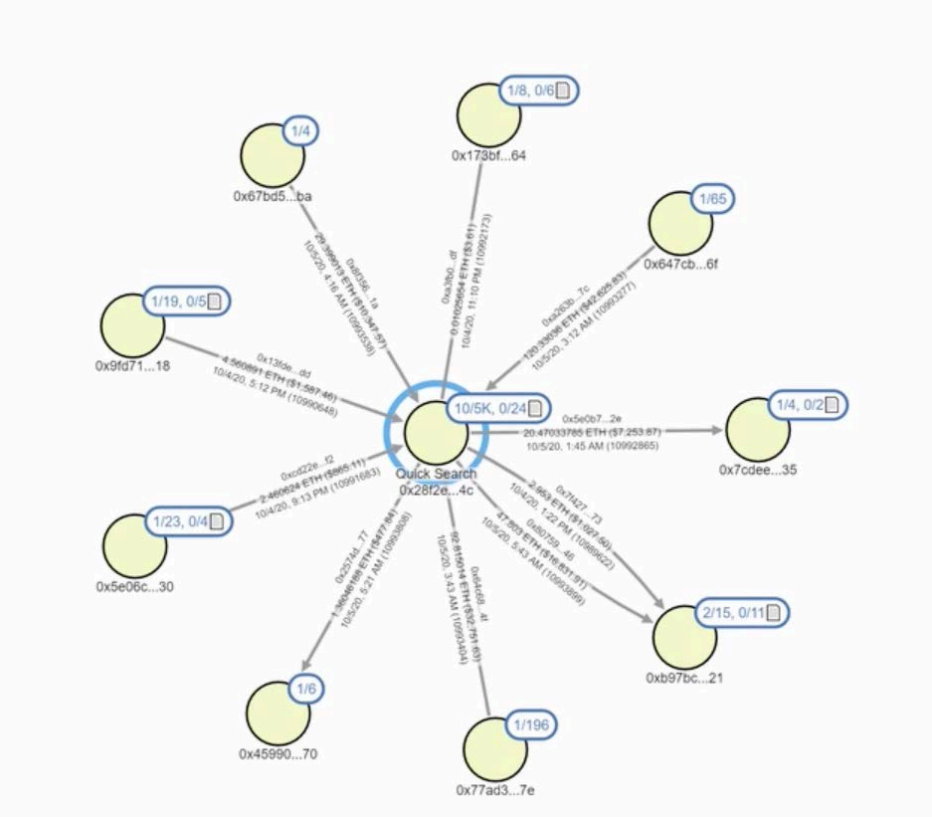
Morgan Stanley

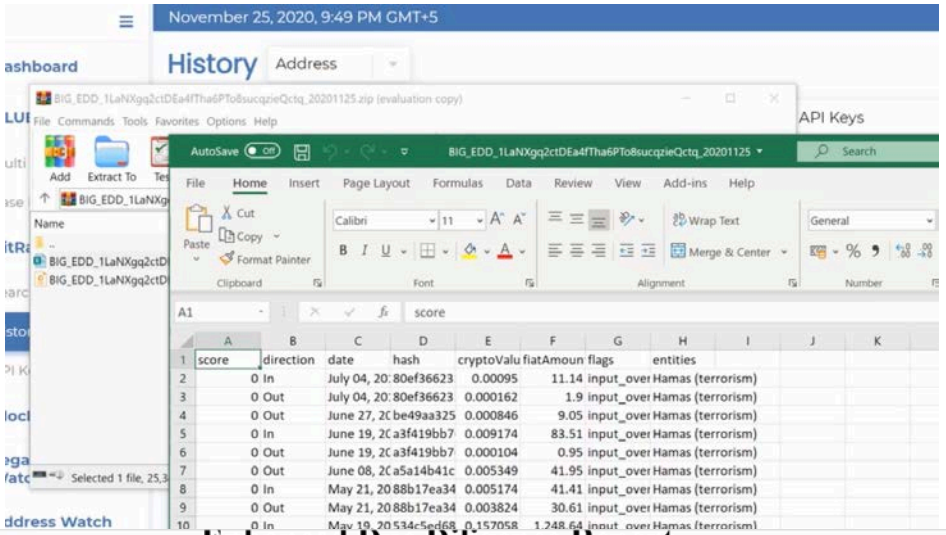
CREDIT SUISSE

Standard Chartered

How can digital assets be tracked?

You can check every wallet or transaction on popular blockchain networks (e.g. BTC, ETH) against blacklists using blockchain analytics tools





Enhanced Due Diligence Report

Bitcoin address: 1LaNXgq2ctDEa4fTha6PTo8sucqzieQctq

BitRank® Score: 0

This **Bitcoin Address** returned a score of **0**. The score for this address is a result of associations with **input_over_10k, exchange_client, binance_client_withdrawal, bittrex_client_withdrawal, bitcoinabuse_report, terrorism_financing**. The total number of transactions associated with this address is **4529**. This address has interactions with the following entities: **Hamas (terrorism)**. At the time of this report there were **0.00016772** units of **Bitcoins** with a USD dollar value of **$3.21**. Details of the address and transaction/s associated are listed below.

The scoring range is from 0 to 100, with 0 being the highest risk and 100 being the lowest risk. Scoring is based on Blockchain Intelligence Group's proprietary risk scoring model.

Record keeping

- copies of all documents and information obtained in the CDD process
- supporting records (consisting of original documents or certified copies) in relation to the customer business relationship, including transactions
- threshold and suspicious transaction reports (TTR, STR)
- STR and any relevant supporting documents and information, including internal findings and analysis
- and other documents relating to AML/CFT procedures

should be retained for a minimum period of **six years** from the date of the notification or report, termination of the business relationship or completion of the transaction, whichever is the later.

Communications with the regulatory Authorities

- AIFC's Financial Services Regulatory Committee conducts an annual thematic review of participant compliance
- Receive advisory support from the Committee
- Joint discussion and development of ML/TF methodologies in digital assets
- Receive advice on a regular basis from AFM (methodological support in qualifying threshold and suspicious transactions)
- Advice on preparation for national assessment

Financial literacy for digital assets

- The Company is actively working to improve financial literacy in digital assets among the public in both the Kazakh and Russian languages.

5
Articles in national media

17
TV appearance

Mini-Courses on Investing
6 video lessons

Regular podcasts and live social media broadcasts with financial and tax advisers

Digital assets and Islamic finance standards

- In cooperation with the «Shariyah Review Bureau» consulting agency, a new investment product, «QuantDART Halal Fund», has been developed and approved, which is unparalleled in the CIS.
- The product is aimed at long-term capital appreciation against the US dollar.
- It is a good start for initial investment in digital assets for people of the religion of Islam.
- Active outreach to the target audience is underway

QuantDART

Common fraud schemes

- The most common digital asset fraud scheme remains - the taking of digital assets in the course of an exchange. (OTC/P2P).
- There are also instances of digital assets being transferred to unlicensed brokers.
- Using "fake" websites of well-known crypto exchanges

QuantDART

Conclusion

- Undertake a comprehensive approach aimed at:
- Increase knowledge about the world of digital assets.
- Develop rational, saving and saving behaviour towards digital assets.
- Provide a constant reminder of the risks involved in investing in digital assets.
- A focus on socially vulnerable populations.

Increasing the financial literacy of the clients as a mechanism for reducing the risks of money laundering and terrorism financing

Presentation By:

State Bank of India

Measures taken by SBI for raising awareness of clients on the risks of their abuse for ML/TF, fraud and other illegal activities

➢ Direct Communication with clients

- **Engaging CSP** (Customer Service Points) in creating client's awareness while onboarding. The customers dealing with CSP are mostly illiterate and underserved in getting the financial services therefore most vulnerable for being used as Money Mules and various frauds.
- **Session in R-SETI (Rural Self Employment Training Institutes)** : Ministry of Rural Development (MoRD) conducts training programmes for rural youth to take up self-employment/ entrepreneurship ventures with the support of sponsor bank. SBI is sponsoring 152 R-SETI across the country and we engaged with rural participants in the training programmes and conducted sessions to make them aware of the fundamentals of ML/TF, modus operandi of money laundering and terror funding and prevention thereof, by adopting suitable precautions. The idea behind this initiative was to create awareness among rural population, especially those aspiring to start small businesses regarding the vulnerability of misuse as money mule accounts.
- **Session in FLCs (Financial Literacy Centers) :** Sessions similar to R-SETI are also being conducted in the Financial Literacy Centers sponsored by SBI.
- Creating awareness towards a safe banking environment by **visiting various Housing complexes**
- Conducting **Walkathon and Skits** at prominent public places and in big branches on various best banking practices and DO's and DONT's to be followed by the client's.

Measures taken by SBI for raising awareness of clients on the risks of their abuse for ML/TF, fraud and other illegal activities

➢ Use of Banking Channels & Services

- A video on ML/TF Risk & Cyber Security is displayed on Bank's ATM screens.
- SMS to Bank customers at frequent intervals at least once in a month on ML/TF risk and cyber security.
- A cyber–Security Page is introduced on SBI's corporate website (bank.sbi) to educate customers about the best practices making them aware of the modus operandi of social engineering frauds such as phishing, smishing, vishing.
- Sending leaflets on DOs and DONT's to customers through emails recorded in their account opening forms.
- Printing of Security Tips on passbook for customers
- Banners are displayed on Bank's internet banking website and bank's public facing websites for customer education.
- Videos and static posts are displayed at branch display system for customer education. This also includes Do & Don't list displayed in all branch premises.

Measures taken by SBI for raising awareness of clients on the risks of their abuse for ML/TF, fraud and other illegal activities

➢ Use of Media & Advertising

- Social Media Posts on Cyber Security
- Multilingual Radio Jingles on Cyber Security for broadcast on FM & AIR stations
- Publishing & distributing small infographic booklets on ML/TL Risk and Cyber Security covering information on various technique employed by the fraudsters for getting financial credential like user ID password and card details and commonly seen cyber frauds**.**
- Cyber Security and ML/TF Risks banners and Hoardings are displayed at prominent public places such as Airport, Railway Stations, Bus stand and other important places to draw the attention of the people towards Cyber Security & ML/TF Risks

HDFC BANK
We understand your world

EAG meet of International Compliance Council
(Wednesday – 25th May 2022)

Initiatives Undertaken

The Bank focuses on the following aspects to increase the Financial Literacy of its customers:

- Internal - Staff education and training.
- External - Outreach program to customers.

Internal: Education / Training programs aimed at enhancing the staff awareness on AML-KYC and related matters.

- E-learning trainings: KYC - AML / CFT Training.
- Trainer led online courses focusing on building a strong line of defense across the bank.
- Knowledge Series mailers aimed to build awareness on Frauds, Attempted / Suspicious Transaction Reporting etc.

A vigilant bank official not only acts as a deterrent to safeguard the bank from being used as a conduit for ML / TF purposes, but also helps protect the interest of the customers (existing or potential) by building risk awareness:

- To not share copies of KYC documents with strangers.
- To not respond to messages offering / promising prize money, government aid and Know Your Customer (KYC) updation receive prize money from banks, institutions etc.
- To ensure the customer is not used as Mules by fraudsters to route illegal / illicit money via their accounts.
- To ascertain the identity and details of the person contacting them prior to sharing any confidential information.

Copyrights © HDFC Bank - Restricted

External Outreach program to customers

Awareness Campaigns conducted to enhance the Financial Literacy of Customers:

- Print & Digital Media campaigns covering 100 million+ individuals.
  (70+ Articles | 20+ States and Union Territories | 10+ Regional languages)
- 2800+ Workshops covering 0.1 million + Individuals creating Digital Awareness – Do's & Don'ts.
  (Target Segment – Youth of India 620 workshops covering 60K+ students)
- 100+ Awareness Campaigns conducted during FY'22.
  (Covering Customers & Employees - Channelized through Social Media & Bank Channels)
- ATM Screen Savers & Digital Displays (14,100 ATMs and 2138 Screens)
- Collaboration with NPCI focussed on UPI Frauds. (Awareness via Social Media and Mobile Notifications)
- Mobile Banking – SMS Push Notification (Coverage: 2.5 million)

Copyrights © HDFC Bank - Restricted

THANK YOU

Copyrights © HDFC Bank - Restricted

Financial Literacy in Securities Market in India

International Compliance Council workshop – Eurasian Group (EAG)

Background of SEBI and its Intermediaries

- The Securities and Exchange Board of India is the regulator of securities market in India.
  - to protect the interests of investors in securities market and
  - to promote the development of, and
  - to regulate the securities market and for matters connected therewith or incidental thereto.

- As mandated by Prevention of Money Laundering Act, 2002 , SEBI laid down guidelines to the market participants for mitigating the risks of money laundering and raising awareness among its market participants.

Major private sector participants in securities market

- Stock Exchanges:
  - BSE Ltd.
  - Metropolitan Stock Exchange of India Ltd.
  - Multi Commodity Exchange of India Ltd.
  - National Stock Exchange of India Ltd.
  - National Commodity & Derivatives Exchange Ltd..

- Depositories:
  - Central Depository Services Ltd
  - National Securities Depository Ltd.

- Mutual Fund Industry through AMFI (Association of Mutual Funds of India).

KYC (Know Your Customer) as a tool of mitigating money laundering

- KYC is the process of identifying and verifying the client's identity when commencing an account based relationship.
- Uniformity in the KYC requirements for the securities mark investors.
- Permanent Account Number (**PAN**) is used as a uniqu identifier in the securities market transactions.
- There is a centralized system of KYC registration agencies t facilitate storing, safeguarding & retrieving investors KYC information and to maintain uniformity of data across intermediaries
- They also help in dissemination of KYC information to the intermediaries as and when required .

Mandate to have 6 KYC attributes in securities market

- The KYC components are:
  - Name,
  - Address
  - PAN,
  - Mobile No,
  - Email ID,
  - Income Range.

- In Indian securities market , there are approx. 95 million demat accounts

Investor charter in securities market

- to facilitate awareness among investors about the details of activities carried and services provided by market participants and associated risks including money laundering.
- The Investor Charters inter-alia deals with services provided to investors with timelines and general guidance for Investors which includes Do’s and Don’ts in the securities market.

Investor Awareness Programmes

- These private sector participants have collaborated with SEBI and among themselves to conduct investor awareness programs, workshops and seminars across the country.
  - Visit to SEBI for college and school going students
  - Resource Persons – Financial literacy
  - SMART workshops – for the investors
  - Regional seminars- for financial literacy
  - Investor association workshops

Measures taken by depositories:

- Off market → reason code validation → consideration amount
- We have enlightened the investors to select valid and correct reason code while transferring the shares via Off Market.
- Also guided them to provide consideration amount while transferring shares via Off Market Sale.
- We have also given facility like Easi and SPEEDe for smooth transaction via Off Market.
- SMS alert and physical letters to Investors in case there is any debit transactions in dormant accounts.
- Intimation to the clients via SMS incase any High Value Transaction executed in their account

Key aspects for investor’s awareness programme

- Investors are communicated the list of the ‘Officially Valid Documents’ that will be accepted for the purpose of identification and address verification. A KYC acknowledgement is also issued to investor.
- Investors are encouraged to proactively inform whenever there is a change in KYC information like contact details, address, income, occupation etc. For Enhanced Due Diligence (EDD) on certain category of investors, they are requested to update KYC details and provide additional details on a periodic basis and whenever deemed necessary
- Whenever there is a request for change of bank mandate along a redemption request, we inform the investor that there is a cooling period for the same, as a risk measure. Similarly for change of address, we reconfirm through a physical intimation letter to both the old and current address
- AMFI runs investor awareness campaigns like ‘Mutual Fund Sahi hai’ to promote the concept of an informed investor .

Additional Aspects of KYC

PARTICULAR	RATIONALE
Politically Exposed Persons (PEPs)	Appropriate communication to the investor at time of on boarding on what is a PEP? what constitutes a PEP? Are relatives/close associates also PEP? So that accurate information is provided by investors correct flag is captured by KRAs/RTAs and updated.
Ultimate Beneficial Owner (UBO)	Investors are made aware of the importance of providing correct UBO details/ownership structures so that accounts are not opened in fictitious/benami entities/shell companies
Third Party Payments	Third party payments not permitted, mechanism in place to verify bank details of clients. It is thus ensured that the funds for subscriptions are through a bank account where the first applicant is one of the account holders
Cash	Cash transactions are seldom accepted in the industry, limit is upto Rs. 50,000 per year per AMC. Investors are informed of designated branches where deposit slip can be submitted, which ensures bank account validation. No payouts are done without verifying source of funds
Client's Location (FATF designated 'black list' and 'grey list' countries)	Investors from these countries are apprised of the FATF advisory. Investments are restricted, and where found necessary, additional details are sought for EDD from the investors
SEBI Regulations like pooling of funds	Investors and distributors are apprised of the SEBI circular on discontinuation of usage of pool accounts, which ensures funds are transferred from client's account to AMC collection account
Scheme Information Document (SID)	The SID of Mutual Fund Schemes issued in the interest of the investor speaks about compliance with Prevention of Money Laundering Act (PMLA) w.r.t client onboarding, cash investments, who can invest? etc. A declaration is taken from the investors at the time of any purchase/subscription that they have read and understood the contents of the SID

Distributor Training

- Mutual Fund products are mostly sold and not bought i.e. majority of clients are sourced from brokers/distributors.
- Train the trainer program on AML Related information is conducted by the Regional Service Managers (RSMs) to distributors who in turn will inform the same to the investors
- Training is also conducted on the type of KYC options available, two factor authentication, other Digital Initiatives, MF Central, MFU etc.
- We frequently train our branch personnel on KYC/AML & CFT which also serves as train the trainer initiative as these personnel interact with investors at branches.

Branch Interaction with Investor

- Investors are encouraged not to open multiple folios and multiple bank accounts
- Whenever there is a large discrepancy between invested amount and declared income, we send a communication to the investor to update KYC, if deemed necessary
- Short term redemptions, especially in equity schemes and in a bank account apart from the source account is monitored. Investor is communicated on the risks of such transaction patterns

Enhanced Customer Due Diligence (CDD) policies as an effective Anti-Money Laundering mechanism

- To complete IPV of an Individual investor by way of Video in Person Verification (VIPV) through their App.
- To implement their own Application (App) for undertaking online KYC of investors by taking photograph, scanning, acceptance of OVD through Digilocker,video capturing in live environment, usage of the App only by authorized person of the RI.
- Identification and verification of the persons to know the Ultimate Beneficiary Owner and to obtain, as part of their Client Due Diligence policy, sufficient information from their clients to identify and verify the identity of persons who beneficially own or control the securities account.
- Take all reasonable steps to verify identity of person exercising ultimate effective control over the entity.

Additional Measures taken by stock exchanges for financial literacy

- Investor Charter published on the website of the Exchanges and Stock-brokers covering Rights & Obligation of Investors
- Services provided by Exchanges to Investors
- Guidance to special circumstances related to market activities :
- Investor Awareness created through dedicated campaigns:
- SMS sent to the investors to not fall pray to tips received
- Messages through social media campaign for Assured / Fixed returns
- To update contact details with stockbrokers
- Trade alerts sent to investors through Exchanges
- Investor awareness programs are conducted by the Exchanges across Tier I, II & III cities
- Functionality to report un-solicited messages received

Thank you

INTERNATIONAL TRAINING and METHODOLOGY CENTRE

ITMCFM

for FINANCIAL MONITORING

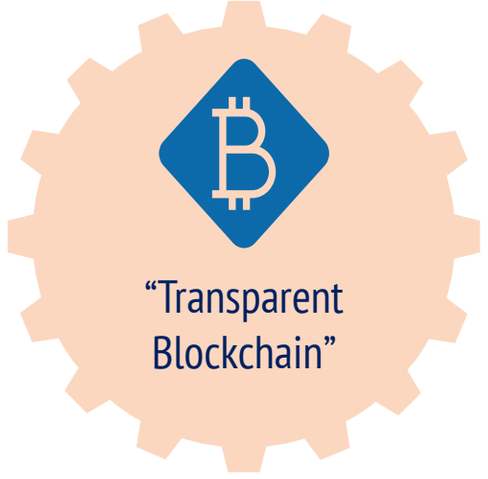
"Graphus" Training System:

Usage Options and Development Prospects

Moscow, 2022

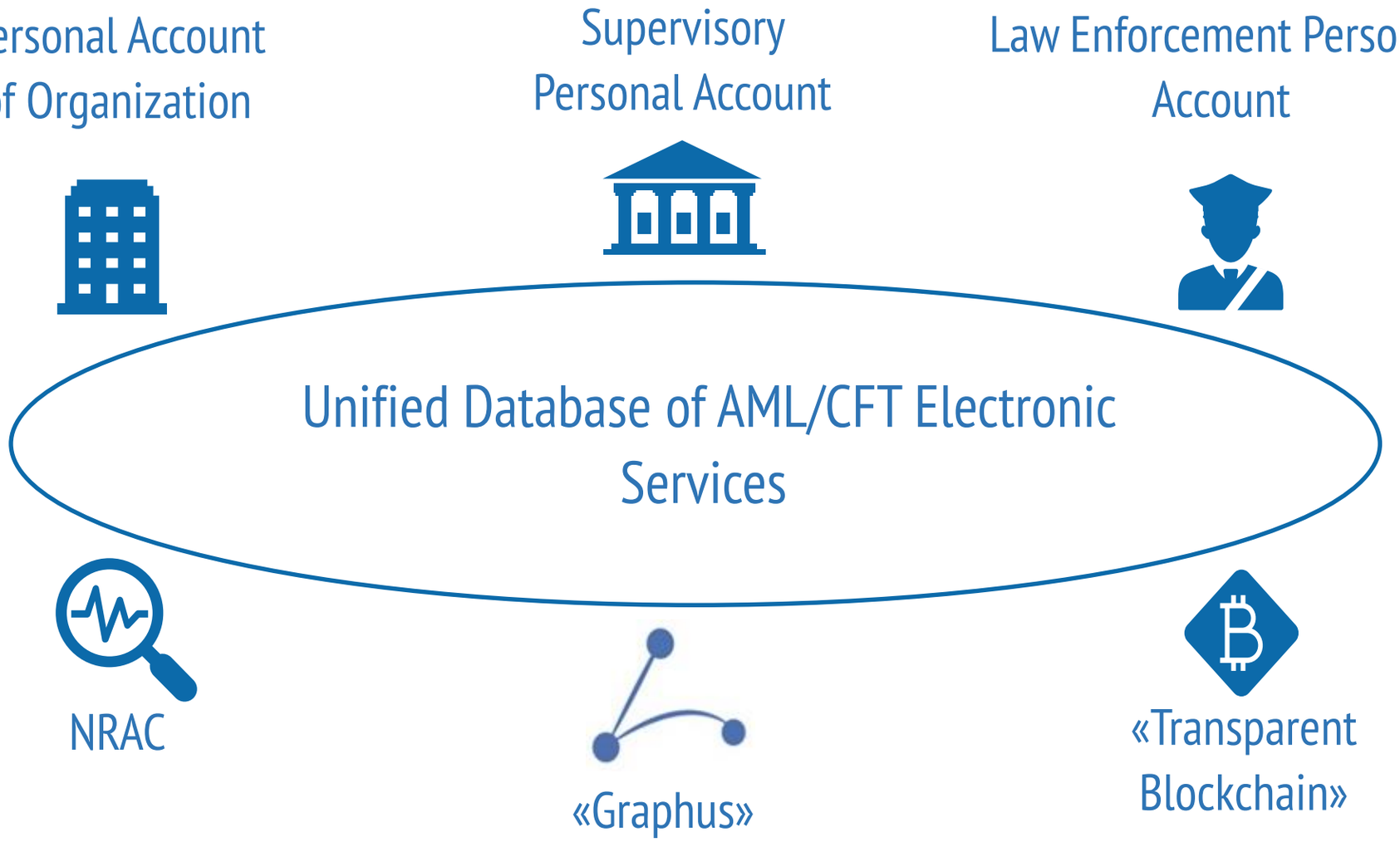
Basic AML/CFT Electronic Services at the ITMCFM Digital Polygon

THE SYSTEM OF INTERACTION BETWEEN THE ANTI-MONEY LAUNDERING SYSTEM STAKEHOLDERS ON THE BASIS OF PERSONAL ACCOUNTS ON THE FIU WEBSITE



MECHANISMS FOR IMPLEMENTATION OF THE FIU FUNCTIONS ON RISK ASSESSMENT AND FINANCIAL INVESTIGATIONS

Educational Ecosystem of AML/CFT Electronic Services



Purpose of Creating the “Graphus” System

- ✓ Financial Investigation Skills Training
- ✓ Conducting AML/CFT Competitions and Tournaments
- ✓ Forming International Training Base of ML/TF Typologies

Main Functional Opportunities of the “Graphus” System

I develop financial investigation cases

II upload knowledge bases which are necessary for conducting the game

III ensure search for and collection of data in the course of the game

IV implement analysis of obtained data

V ensure search for similar precedents to identify typologies

VI provide results, received in the course of the game, via graphical interface

Platforms for Approbation of the “Graphus” System

- Cyber tournament at the International Financial Security Olympiad in October 2021

- Pilot project on approbation at Moscow schools

- Professional development training for teachers of INI’s member-universities and further approbation in a number of universities

- Test conducted by the members of delegations of FIUs of the CIS member states on the ITMCFM platform

Prospective Outcomes of Using the “Graphus” System

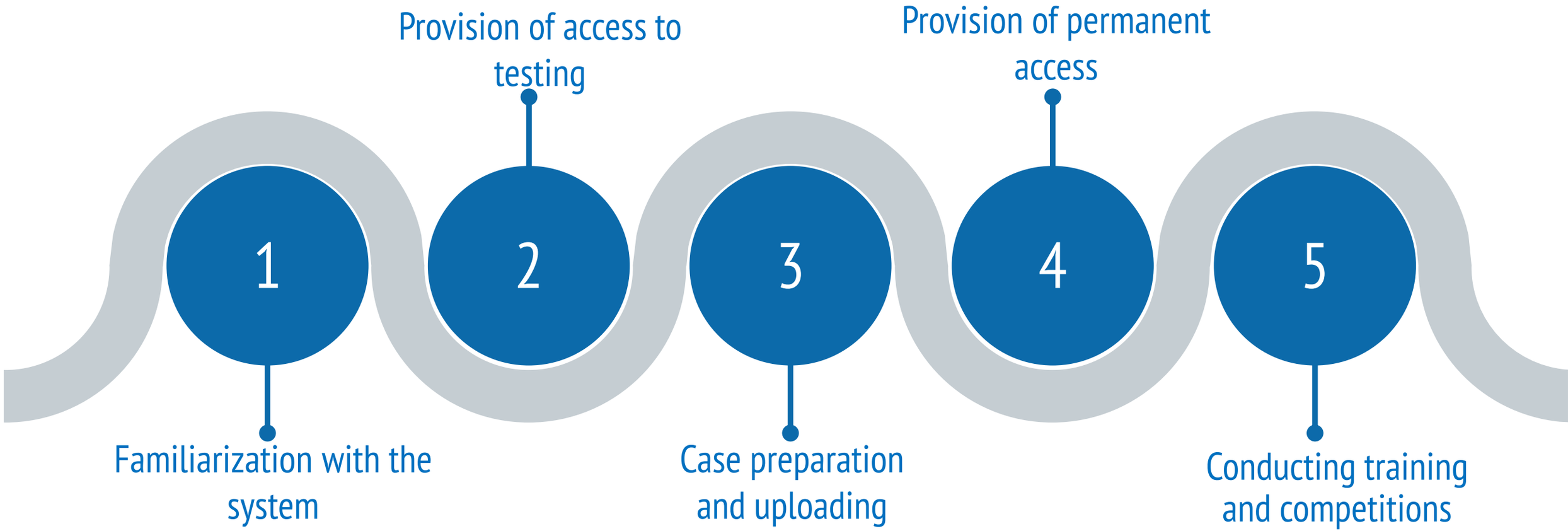
Inclusion in the International Financial Security Olympiad Annual Program

Integration into School Curriculum

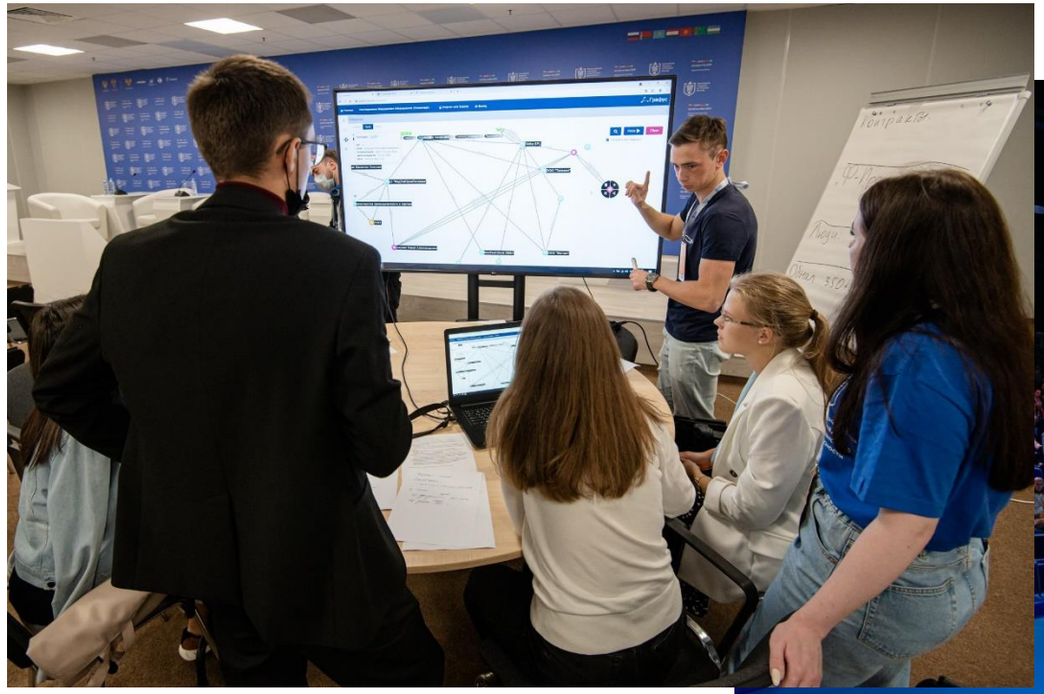
Introduction into the Educational Process of INI’s Universities

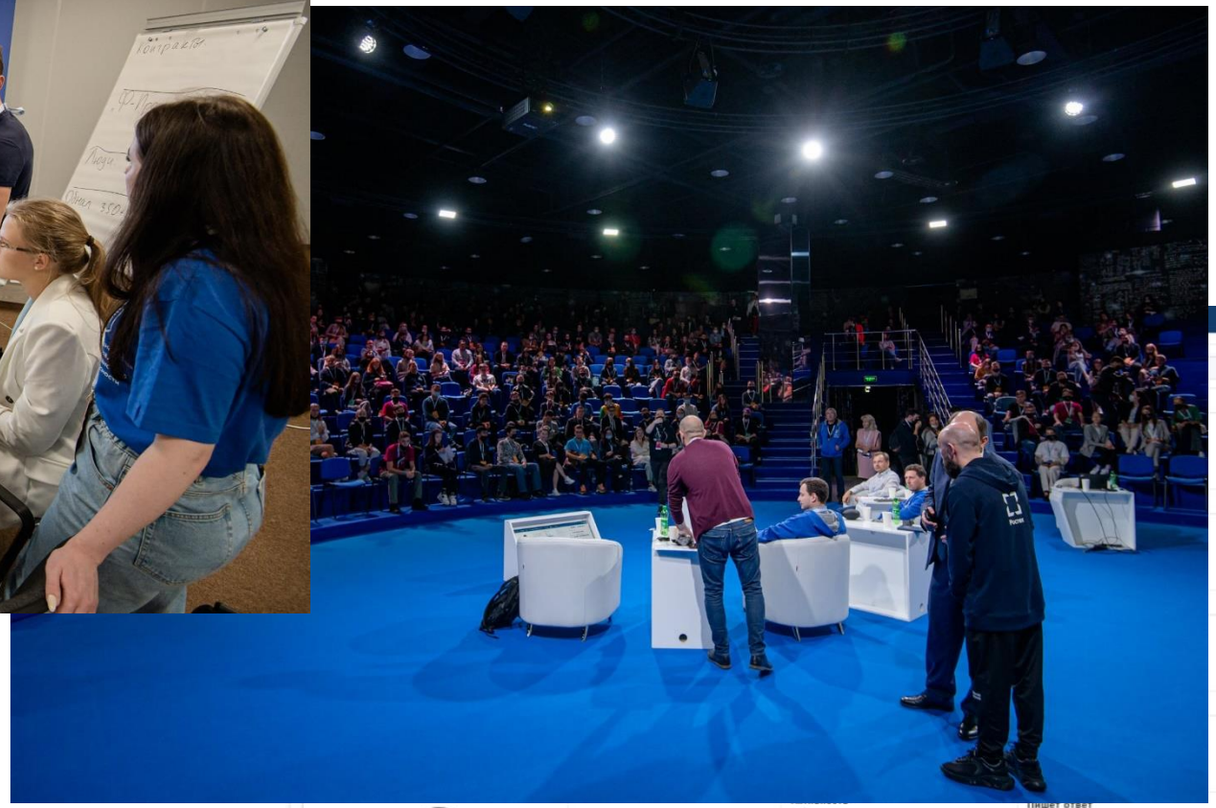
Integration into the Activities of FIUs of the CIS Member States

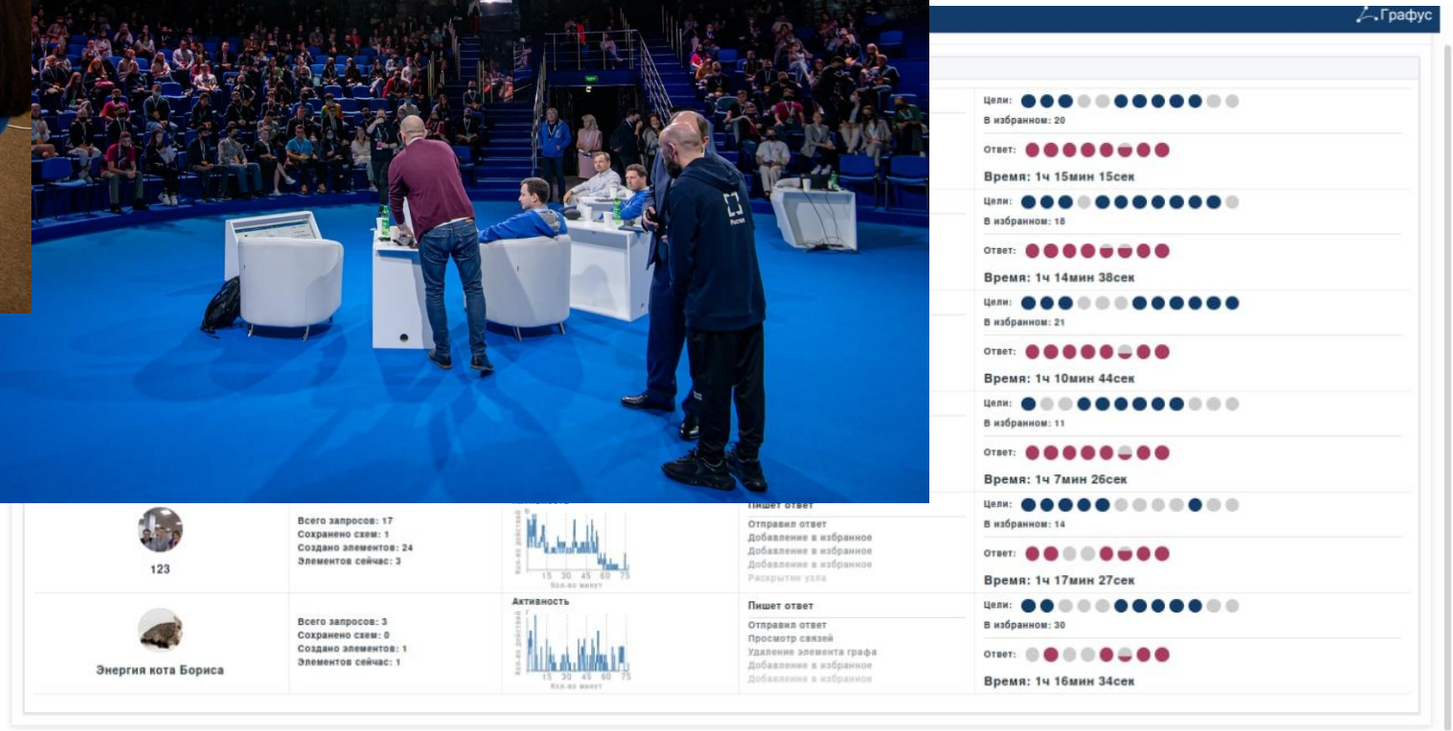
Integration of the “Graphus” System for Primary Financial Monitoring Entities



“Graphus” System at the 2021 International Financial Security Olympiad







INTERNATIONAL FINANCIAL SECURITY OLYMPIAD

May 2022 → **QUALIFYING STAGE**

October 10-14, 2022 → **FINAL STAGE AT THE "SIRIUS" FEDERAL TERRITORY (RUSSIA, SOCHI)**

FORMAT AND TOPICS OF OLYMPIAD EVENTS

- ✓Panel discussions
- ✓Master classes
- ✓Role games
- ✓“Education and Career” exhibition

- ✓Personal financial security
- ✓Financial security of organization
- ✓Cybersecurity
- ✓Personal data security

Central Bank of Turkmenistan and Banks' Policy to Reduce the Extent of Involvement of Customers in ML/TF Schemes

Financial System of Turkmenistan

- Turkmenistan has the two-tier banking system composed of the Central Bank (the first tier), and commercial banks (the second tier)

with 10 operational banks, of which 4 banks are the state commercial banks, including 1 state development bank, 4 banks are commercial joint stock banks, and 1 bank is the branch of the foreign bank

Legal Framework

- Turkmenistan's banks, including the Central Bank of Turkmenistan, do not have correspondent relationships with banks from countries with inadequate AML/CFT system identified by the FATF.
- According to Turkmenistan Presidential Resolution (dated May 30, 2008), Turkmenistan's banks are allowed to carry out transactions involving movement of capital only through the correspondent account opened with the Central Bank of Turkmenistan or with the State Bank for Foreign Economic Affairs of Turkmenistan.
- Current transactions may be carried out through correspondent accounts opened only with the first class foreign banks.
- Branches of commercial banks are prohibited from establishing correspondent relationships (opening correspondent accounts) in foreign currency.

Customer Identification

- According to the applicable regulations, including the Regulation on Bank Account, credit institutions open banks accounts for customers only after full completion of the customer identification process, as required by the FATF Recommendations;

- All documents that allow to identify a customer and also identify and verify customer's representative(s) and beneficiary (beneficiaries) shall be valid as of the date of their presentation;

- All documents presented by customers to credit institutions shall be the originals or duly notaries copies.

* According to the AML/CFT/CPF Law the obliged entities engaged in transactions shall conduct due diligence on customers (their representatives) and beneficiaries:
* 1) when establishing business relations with customers;
* 2) when carrying out transactions with funds and other assets that are subject to mandatory monitoring, including suspicious transactions;
* 3) when there are doubts about the veracity of previously obtained data on customer (customer's representatives) and/or beneficiary.

Customer Identification

- Identification of a customer (customer's representatives) and beneficial owner involves measures taken by an obliged entity (that is subject to financial monitoring) to document and verify identification information on the customer (customer's representative), identify a beneficial owner and document his/her identification data, understand and document the intended purpose of the business relationships or a one-off transaction, and obtain and document other information about the customer (customer's representatives) and beneficial owner as provided for in the relevant regulations

- Measures taken to update and (or) obtain additional information about customers (their representatives) and beneficial owners, including information of the source of funds used by customers for carrying out transactions, and to examine customers' transactions and identify threshold, unusual and suspicious transactions.

* **ML/TF Risk Factors:**
* **Country (geographic) risk**
* Credit institutions need to know and take into account the following: in what countries their customers are registered; where their head offices are located; nationality of their customers; and where they conduct their core business.
* **Customer risk**
* These categories of customers include, in particular, individuals, financial institutions and legal entities which business activities are exposed to ML/TF risks.
* **Financial product/ service risk**
* Certain products, services , transactions or delivery channels may pose increased ML risk (private banking, cash transactions, non-face-to-face business relationships or transactions, etc.).

Restrictions for Establishing Business Relationships and Carrying out Occasional Transactions and Prohibition of Fake Financial Activities

IT IS PROHIBITED

- **OPEN, MAINTAIN OR PROVIDE**
  - **ACCOUNTS IN FICTITIOUS NAMES AND ANONYMOUS ACCOUNTS**
  - **NUMBERED, ALPHANUMERIC, ETC. ACCOUNTS**
- **ESTABLISH AND MAINTAIN RELATIONSHIPS WITH SHELL BANKS**

PROCESS OF IDENTIFICATION OF PERSONS CARRYING OUT TRANSACTIONS WITH FUNDS

For each group of customers (natural persons, individual entrepreneurs, companies, correspondent banks), a bank develops special customer files, which my be standard and extended.

Extended customer files are completed and maintained in respect of:

- Customers assessed by the bank as posing high level of risk;

- Customers suspected by the bank of carrying out transactions with funds for money laundering and terrorist financing purposes;

- Customers that provide information that raises doubts about it veracity.

PROCESS OF IDENTIFICATION OF PERSONS CARRYING OUT TRANSACTIONS WITH FUNDS

- When establishing business relationships with a first class non-resident bank, banks shall obtain a prior approval of the Central Bank of Turkmenistan and shall also require information on anti-money laundering., counter-terrorist financing and counter-proliferation financing measures implemented by the non-resident bank;

- All documents provided during the identification process, including hard copies of completed questionnaires, are stored with the customer file.

Assessment of Risk Business Relationships with Customer

Based on the information on a customer obtained at the preliminary control stage (i.e. in the process of identification and verification) and also taking into account business activities and transactions posing increased risks, a bank assesses the level of risk of business relationships with the customer and assigns the respective risk rating:

- **Low**

or

- **High**

Corporate Ethics and Prevention of Corruption

- **Law of Turkmenistan on Ethics and Official Conduct of Civil Servants obliges public officials to:**

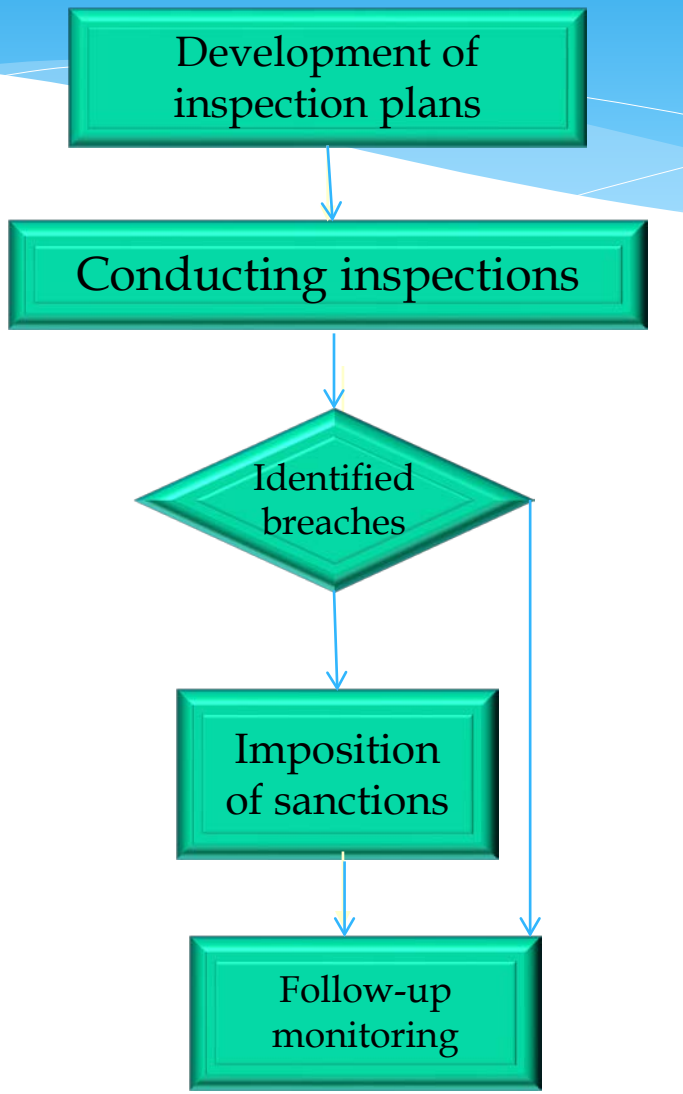
- *Refrain from any actions that may cause doubts about bona fide exercise by civil servants of their functions and duties, and avoid conflicts that may damage their reputation and the image of the government authority;*
- *Comply with the applicable professional code of ethics and code of business conduct;*
- *Avoid any actions driven by personal, financial or other interest that impede bona fide exercise of official functions and duties.*

- Incorporation of compliance culture into the overall corporate culture is a key factor of effective AML/CFT program. Each officer of a credit institution is obliged to exercise reasonable discretion in his/her work and act with integrity and good faith.
- Proper conduct of each officer, including senior managers, should preserve and increase the reputation of a credit institution, which facilitates business growth.

Main Elements of Supervision

- Application of risk-based approach;
- Conducting inspections;
- Assessment, analysis and monitoring of compliance with the internal control rules by supervised entities;
- Methodological support of supervisory activities;
- Interaction with the internal audit departments of credit institutions.

Main Stages of Inspection Process



Main Issues Examined in the Course of Inspection

- ✓ Internal control arrangements, including customer and beneficiary identification and verification procedures;
- ✓ Screening of customers against the list of entities and individuals known to be involved in terrorist activities;
- ✓ Procedure for identification of transactions that are subject to monitoring;
- ✓ Compliance with the requirements and procedures of recording, keeping and reporting information on transactions that are subject to monitoring.

Internal Control System of a Bank Should:

- Prevent intentional or unintentional involvement of a bank in ML/TF/PF;
- Mitigate (reputational, operational, legal, etc.) risks related to possible misappropriation and possible seizure or confiscation of bank's and customers' funds and/or other assets, which may inflict both direct and indirect losses;
- Ensure timely provision of information to the designated government authority as prescribed by the legislation of Turkmenistan;
- Protect confidentiality of records of transactions with funds and persons carrying out such transactions, their representatives and beneficial owners and measures taken by the bank for preventing and identifying ML/TF/PF related transactions.

Internal Controls are Implemented for:

- Identifying all bank's customers carrying out transactions with funds in situations specified by the legislation of Turkmenistan, and keeping records of activities and business reputation of customers;

- Identifying and documenting transactions with funds that are subject to mandatory monitoring, and submitting the relevant information to the designated government authority.

Internal Control Stages

- Preliminary control is performed by way of collecting necessary documents and recording relevant information to develop understanding of a customer (including its beneficial owners), nature of customer's business and expected transactional activity;

- Ongoing control is performed by way of monitoring customer's transaction, taking into account the information obtained by a bank in the course of preliminary control, to identify transactions that are subject to mandatory monitoring;

- Subsequent control is performed by way of analyzing customer's transactions carried out in the past to identify suspicious transactions, conducted over a long period of time and unidentifiable at the stage of on-going control, that should be subject to mandatory monitoring.

Internal Control Rules shall Include the Following Programs:

* 1) AML/CFT/CPF internal control program;
* 2) ML/TF/PF risk management program that takes into account customer risks and risk of misuse of products and services, including new technologies, for criminal purposes;
* 3) Customer identification program;
* 4) Program of monitoring and examining customers' transactions, including complex, unusually large and abnormal transactions;
* 5) Program of AML/CFT/CPF training of staff of obliged entities (engaged in transactions);
* 6) Other programs that may be developed by obliged entities (engaged in transactions) in compliance with the internal control rules.

Sanctions for Non-Compliance with the Statutory Requirements

- In case of breach by a credit institution of the legislation of Turkmenistan and the relevant regulations of the Central Bank of Turkmenistan, the following enforcement measures can be applied: written warning and order to eliminate committed breaches; fine in amount of up to 0.1% of the minimum authorized capital or restriction to carry out certain types of banking transactions for up to six months; suspension and/or cancellation of the credit institution's license;

- Natural and legal person as well as executive officers of the government authorities are held liable (for improper fulfillment of their respective duties and obligations) under the Code of Administrative Offences of Turkmenistan for breaches of the provisions of the AML/CFT/CPF legislation of Turkmenistan committed by obliged entities and licensing authorities.

Thank you for attention!!!