



EAG



INTERNATIONAL WORKSHOP

"Public-Private Partnership as a Tool to
Improve the AML/CFT System"

Consultations with the private sector

PRESENTATIONS' DIGEST

26 - 27/09.2019

KAZAN/RUSSIAN FEDERATION



Council of Europe
Conseil de l'Europe

IO.3 and IO.4 Current Assessment Practices

OVERVIEW

Kotryna Filipaviciute

Administrator at the MONEYVAL Secretariat

Council of Europe
Conseil de l'Europe

Immediate Outcome 4: preventive measures applied by the private sector

Assessing the application of preventive measures and supporting the conclusions on Core Issues:

- Level of compliance with recommendations 9-23 and elements of 1, 6 and 29;
- Increased focus on specific sectors (in accordance with the risks and contextual factors)
- The selection of reporting entities based on an analysis of institutional data and information provided by the supervisory authorities

- **On-site interviews serve as a basis for assessing IO 4;**
- **The conclusions has to be supported by other sources of information**, such as:
 1. Internal AML/CFT policies
 2. Supervisory data: a) offsite data: sectorial/ institutional risk assessments; b) on-site data (comprehensive supervisory findings, statistics, severity of the breaches, etc.)
 3. The NRA findings
 4. STR reporting trends and practices, etc.

Core issue 4.1

How well do reporting entities understand ML/T risks and obligations? (I)

To what extent have the NRA results been taken into account?

NRA



BRA

- Country's risk exposure - National Risk Assessment (NRA);

- Firm's risk exposure - Business Risk Assessment (BRA)

Core issue 4.1

How well do reporting entities understand ML/TF risks and obligations? (II)

1. Country's risk exposure - National Risk Assessment (NRA)

- NRA findings (incl. NPOs, legal persons and legal arrangements, virtual assets, TF related risks, etc.)
- to what extent are the NRA results used to increase the understanding of risks, threats and vulnerabilities?

2. Sectorial risk assessment, supranational risk assessment (if any)

3. Firm's risk exposure - Business Risk Assessment (BRA)

- main risks, threats and vulnerabilities
- risk mitigation plan
- allocation of resources/responsibilities and monitoring (incl. involvement of senior management)
- BRA update/renewal (frequency, scope, trigger events)

Core issue 4.1

Are controls commensurate with the risks?

Examples:

Corruption

- **Focus on PEPs**
- stricter PEP controls (foreign PEPs vs. domestic PEPs);
- specific focus on close associates and BOs;
- specific monitoring scenarios, etc.

Prevalent use of cash

- **Focus on cash transactions and customers engaged in cash intensive businesses**
- reduced thresholds;
- stricter monitoring scenarios for cash deposits/withdrawals and currency exchange in cash), etc.

Tax evasion/ sanctions evasion

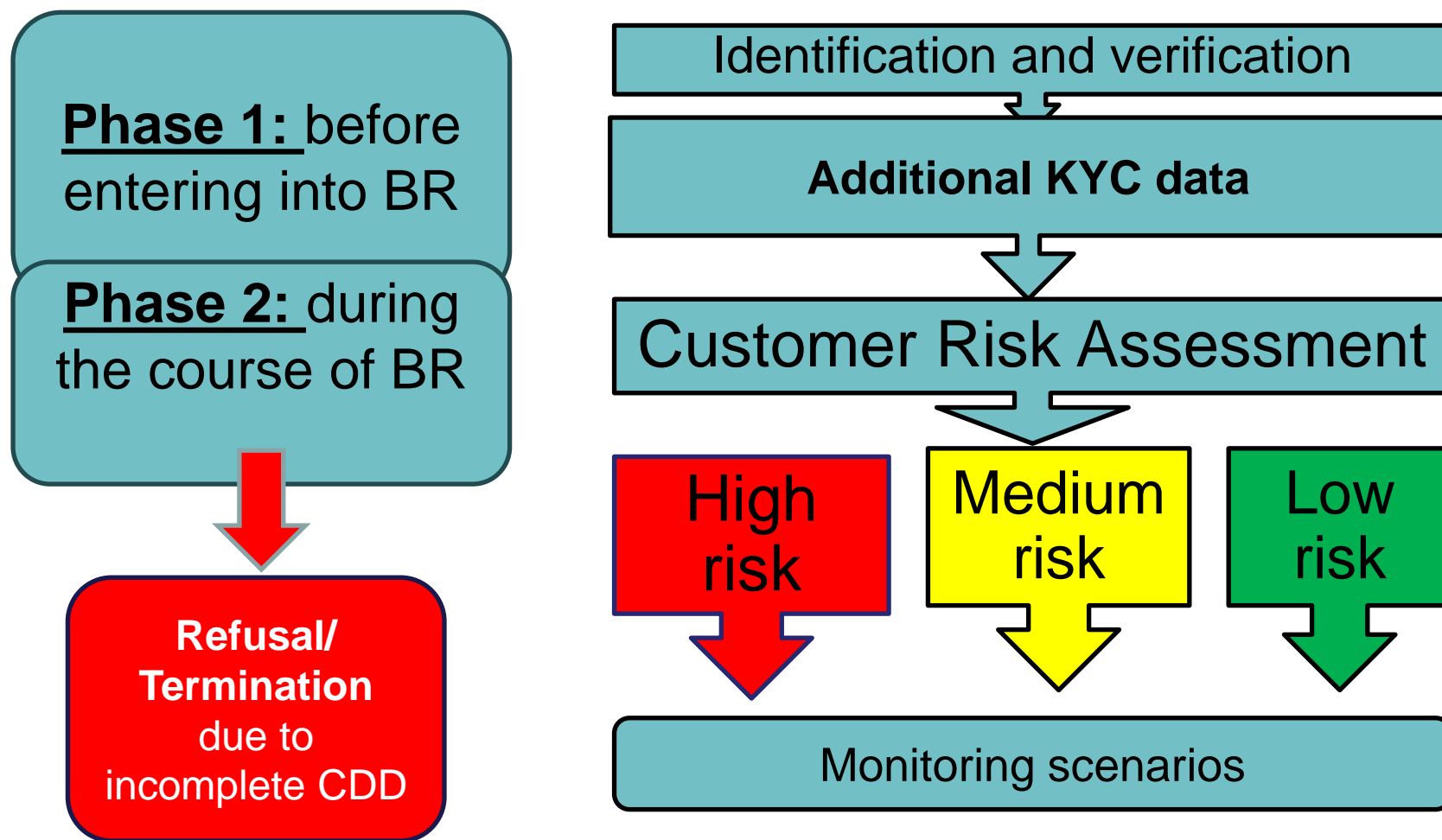
- **Focus on legal persons and legal arrangements, etc. (e.g. large share of legal persons with complex ownership structure in entire customer database) , their transactions/business partners**
- stricter BO controls (incl. extensive ownership data);
- monitoring scenarios in line with customer's business and risk profile;
- targeted training for employees, etc.

Core issue 4.3 CDD and record keeping

Areas to be assessed (R. 10,11, 17, R.22-23):

1. Identification and verification of the customer and BO
2. Purpose and nature of business relationship (BR)
3. Customer risk assessment (CRA) – risk profile
4. Refusal to enter into business relationship (BR) due to incomplete CDD; refusals that resulted in STRs (criterion 10.19)
5. Monitoring
6. Record keeping
7. Termination of the BR due to incomplete CDD; terminations that resulted in STRs (criterion 10.19)
8. CDD renewal (frequency, scope, RBA)

Core issue 4.3
CDD and record keeping:



Core issue 4.3

CDD and record keeping:

Poor practices:

- BO identification concerns (complex legal structures, legal arrangements, nominee shareholders, bearer shares, etc.);
- Purpose and nature of BR is not clear or justified (e.g. non-resident customers);
- Customer risk assessment does not fully take into account all relevant factors (risks related to geographical factors, delivery channels, products, services, transactions, customer's business, etc.);
- Little consideration is given to the customer risk assessment during the course of BR (e.g. no specific criteria to re-assess the risk; no specific or enhanced measures applied when customer's risk level changes from low/medium to high and from high to lower risk level);
- Monitoring scenarios are not developed in accordance to the customer's risk level, i.e. no specific/enhanced monitoring scenarios for high risk customers; no distinction between monitoring of low and medium risk customers, etc.
- Refusal to enter into BR or termination of BR due to serious ML/TF considerations do not result in the submission of a STR;
- No enhanced monitoring of the BR after the submission of a STR;
- CDD to existing customers is not performed following the risk based approach (e.g. frequency of CDD updates and scope of KYC/CDD information is not being determined on the basis of customer risk)

Core issue 4.3

Failure to satisfactorily complete CDD

Additional clarifications, as requested by the workshop participants

Recommendation 10, criterion 10.19:

Where a financial institution is unable to comply with relevant CDD measures:

(a) it should be required **not to**

1. open the account,
2. commence business relations
3. or perform the transaction;

• **or should be required to terminate the business relationship;**

(b) it should be required **to consider making a suspicious transaction report (STR)** in relation to the customer.

** DNFBPs are required to comply with the requirements of the recommendation 10; see Recommendation 22: “DNFBPs: customer due diligence”*

Core issue 4.4 Enhanced and Specific CDD

Areas to be assessed:

1. PEPs controls (R.12, R.22)
 2. Correspondent banking and other similar relationships (R.13)
 3. New technologies (R.15, R.22)
 4. Wire transfer rules (R.16, R.14, in particular c.14.4-14.15)
 5. TF-related TFS (R.6, c.16.18)
 6. Higher-risk countries identified by the FATF (R.19, R.23).
- * DNFBPs: R. 22-23

Core issue 4.4

Enhanced and Specific CDD

PEPs (I)

Areas to be assessed:

- Level of compliance with R.12 (technical deficiencies)
- Scope of EDD measures (domestic vs. foreign PEPs); purpose of entering into the BR with foreign PEPs
- Checks to verify PEP status (self-declaration of the customer + verification using reliable sources):
 - at the on-boarding stage
 - during the course of BR
 - frequency and scope of the checks (customer, BO, representative; directors; ownership chain)
- Identification of the family members and close associates of PEPs;
- Enhanced monitoring (specific scenarios)
- Other enhanced CDD measures (senior management approval, SoF, SoW, etc.)
- Obtaining information on:
 - Source of wealth (SoW)
 - Source of funds (SoF)

Core issue 4.4 Enhanced and Specific CDD **PEPs (II)**

Poor practices:

- purpose of entering into the BR with foreign PEPs is not clear;
- no processes/procedures in place to identify family members and close associates of PEPs (e.g. no customer self declaration obtained, excessive reliance on commercial databases, no checks in relation to the close associates of PEPs during the course of ongoing monitoring, i.e. closer look at transactional parties, business partners, etc.)
- No processes in place to identify, whether the existing customer became a PEP (during the course of BR)
- Scope of checks to verify PEP status is too narrow (e.g. no checks on BOs, incl. directors)
- No enhanced monitoring applied in relation to PEPs (or specific monitoring scenarios developed)
- Monitoring scenarios designed for foreign vs. local PEPs do not differ (relevant, when the purpose of BR with a foreign PEPs is not be clear or justified)
- No distinction between SoW and SoF (poor understanding).

Core issue 4.4

Enhanced and Specific CDD

Correspondent banking

Risk and materiality:

- Statistics (correspondent banking relationships and volume of funds transferred)
- Countries of establishment of the respondent banks
- Other types of correspondent relationships

CDD measures:

- Level of compliance with R.13 (impact on practical application)
- Specific CDD measures

Core issue 4.4

Enhanced and Specific CDD

New technologies

Areas to be assessed:

- Level of compliance with R.15
- Is assessment conducted prior to the launch of new products/services/ technologies/ delivery mechanisms?
- Is assessment carried out on an on-going basis?
- What are the main risks and mitigating measures?
- **! EXAMPLES**

Poor practices:

- DNFBPs are less aware of the requirement / do not conduct such a risk assessment (however, judgement has to be based on the nature of services that reporting entity provide and technologies that they use (if any))
- FIs' risk assessments in relation to new technologies are generally linked to operational risk assessments, with a very little emphasis, if any, given to ML/TF risks.

Core issue 4.4

Enhanced and Specific CDD

Wire transfers

Risk and materiality:

- Statistics (main countries involved in transfer of funds (origin/destination); volume of funds transferred).

Application of wire transfer rules (areas to be assessed):

- Level of compliance with R.16
- Scope of the information that accompanies transfer of funds
- Procedures to detect missing information
- Measures taken in accordance with RBA (restriction/closure of BR with PSP of the payer, intermediary PSP; STRs filed)
- Internal control in relation to the agents of the MVTs provider
- TFS and higher risk countries.

Core issue 4.4 Enhanced and Specific CDD **TF-related TFS**

Areas to be assessed:

- **Screening procedures: the nature, scope and frequency of checks:**
 - at the time of on-boarding
 - during the course of BR
- **Sanction hits and reporting procedures**
- **Handling of false positives**

Poor practices:

- screening is performed on an occasional basis (the frequency of screening checks is determined based on the customer's risk level);
- scope of screening checks is not sufficient (e.g. in case of complex legal structures and legal arrangements;
- no procedures to detect close associates of sanctioned entities/persons and /or persons having direct and indirect links with the sanctioned persons/entities; no emphasis on monitoring/screening of the parties of transaction.

Core issue 4.4

Enhanced and Specific CDD

Higher-risk countries identified by the FATF

Risk and materiality:

- Volume of funds originating from high risk countries; Volume of funds transferred to high risk countries
- Number of clients and BOs from high risk countries (place of residence, citizenship, nationality);
- Scale of activities related to high risk countries.

Application of enhanced and specific measures:

- Specific CDD measures applied with respect to the customers having links with high risk jurisdictions (examples)
- Specific CDD measures applied with respect to transactions originating from high risk countries/ transferred to high risk countries

Poor practices:

- Stricter controls implemented by the reporting entities with respect to the customers that reside in higher risk countries, however, no specific measures applied with respect to the transactions to/from higher risk countries (e.g. no specific or enhanced monitoring scenarios).

Core issue 4.5

Reporting obligations (I)

Areas to be assessed:

- Internal STRs vs. STRs filed to the FIU
- Reporting of attempted transactions
- Monitoring scenarios to identify suspicious activities linked to: a) TF; b) ML

Poor practices:

- Number of internal and external STRs in smaller FIs and DNFBPs does not differ significantly which puts into question the effectiveness of monitoring; (to be assessed taking into account the nature, size and scale of business activities and clientele of the reporting entity)
- No specific (or very little) monitoring scenarios to identify TF; TF is understood to a lesser extent than ML
- Lack of understanding of TF and ML-related typologies (in particular sector specific)
- Monitoring is limited to transactions' checks; very little emphasis on customer behaviour (retrospective monitoring) and parties of transaction
- Low level of reporting (smaller FIs and DNFBPs)

Core issue 4.5

Prevention of tipping-off (II)

- Are practical measures to prevent tipping-off in place? Is this (and if so, how) reflected in AML/CFT training programs?
- Any issues in the past? (e.g. disclosure of the sensitive information; issues with the delayed transfer and communication with the customer, etc.)
- Is FIU feedback prompt enough to eliminate tipping-off concerns? (see also R. 20-21)

Core issue 4.6

Internal controls

Areas to be assessed:

- Allocation of responsibilities (3 lines of defence: front, AML, compliance and audit function)
- Risk management and internal control (involvement in senior management in AML/CFT matters, management reporting, monitoring, communication, decision making, etc.)
- AML/CFT training programs (staff training)
- Group wide policies and procedures, etc.

Immediate Outcome 3: SUPERVISION

Assessing the supervision, monitoring and regulation of FIs and DNFBPs and supporting the conclusions on Core Issues:

- Level of compliance with recommendations 14, 26, 27, 28, 34 and 35 (and elements of recommendations 1 and 40)
- Increased focus on specific sectors (in accordance with the risks and contextual factors; NRA findings, sectorial risk assessment data, etc.)

The conclusions on Core Issues has to be supported by other sources of information, such as:

1. Size, composition and structure of FI and DNFBP sectors
2. Licencing processes
3. Supervisory data: a) offsite data: sectorial/ institutional risk assessments; b) on-site data (comprehensive supervisory findings, statistics, severity of the AML/CFT breaches, etc.)
4. Supervisory manuals (off-site assessments, on-site checklists, documents outlining how the risk rating of the supervised institution drive scope and frequency of future supervisory actions)
5. Awareness raising initiatives (guidelines, manuals, trainings, seminars), etc.

Core issue 3.1

Licencing/registration and other controls

Areas to be assessed:

- Level of compliance with R.14, R.26 and R.28

New applicants:

- Fit and proper tests (scope, depth and frequency; criteria, factors; cooperation with relevant authorities; persons subject to checks; criminal, reputation checks; supporting data and documentation, SoW, etc.)
- Assessment of wider ML/TF risks (risk profile of the applicant, business model, geo risks, negative info, etc.)
- Decision for granting/ refusing the licence
- Close associates of criminals (checks)
- Statistics (licence applications received / refused/ withdrawn / granted – reasons of withdrawals, refusals, etc.)

Licencees:

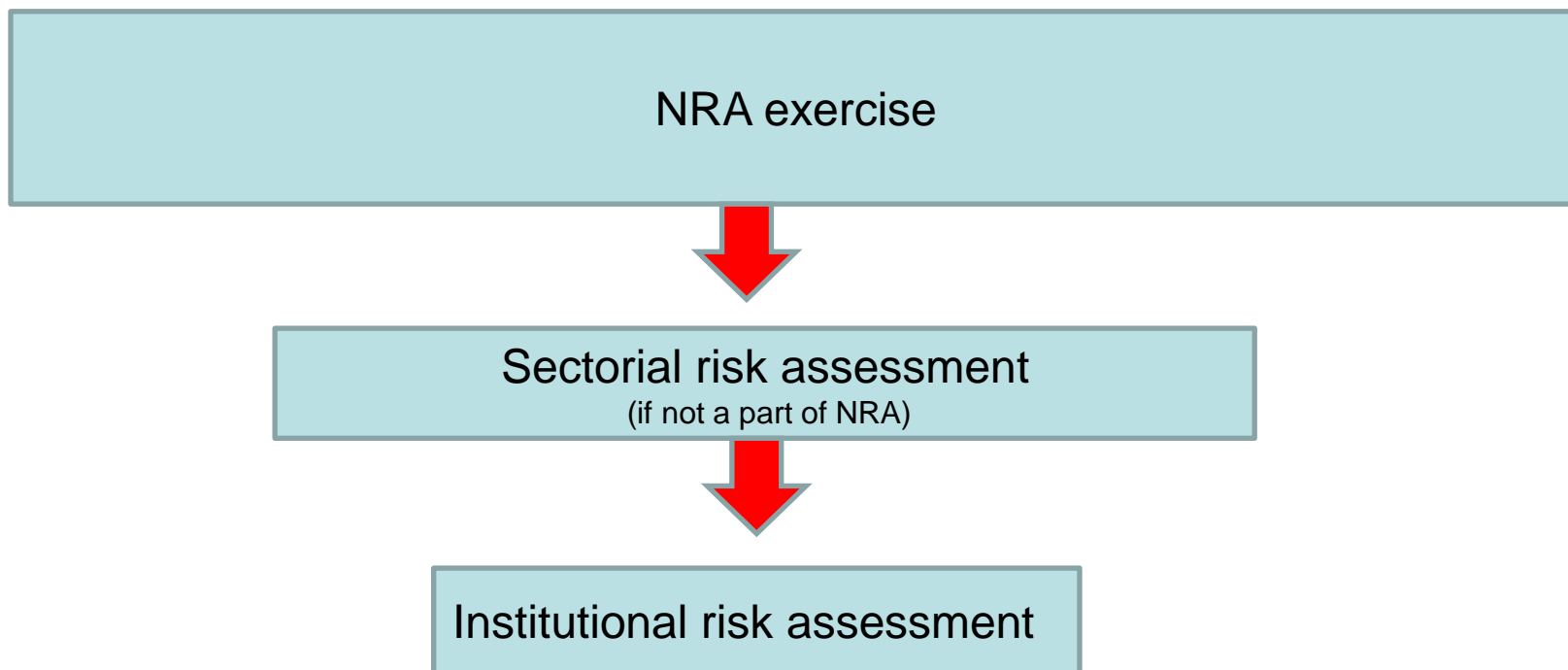
- Amendments to the existing licence
- Change in shareholding; qualifying holding
- Appointment of key function holders
- On-going monitoring (for licence holders)
- Statistics (withdrawn licences, reasons, etc.)

Other factors:

- Exemptions, unregulated sectors
- Un-licensed activities

Core issue 3.2

Understanding of the ML/TF risks by the supervisors



Core issue 3.3

Risk-based supervisory processes

- Level of compliance with R.26-28, R.14
- supervisory resources, supervisory powers
- off-site supervisory tools and practices, adequacy of sectorial and institutional risk assessments (scope, frequency, criteria)
- how does the risk level of the subject person drive the scope and the frequency of the future supervisory actions?
- on-site supervision (methodologies, on-site planning, inspection and post-inspection processes)
- cooperation with relevant competent authorities (domestic and foreign); group wide supervision
- Examples of the supervisory measures: off-site reviews, thematic reviews (both onsite and offsite), targeted inspections, full scope inspections, meetings with the key function holders (e.g. AMLCO, management), other forms of engagement with the private sector.

Is the supervision risk based? How can supervisors demonstrate it?

Core issue 3.4

Sanctions for AML/CFT breaches

- Level of compliance with R.35
- Sanctions application policy
- Decision making process (protected from undue influence, clear criteria, etc.)
- Effectiveness, proportionality and dissuasiveness of sanctions (severity of the breaches, etc.)
- Sanctions imposed:
 - On the basis of onsite findings
 - Other (e.g. breaches of licencing requirements), etc.
- Examples of the follow-up actions
- Criminal sanctions (incl. cases submitted to LEAs, if relevant, etc.)
- Sanctions for STR reporting-related violations
- Sanctions for tipping-off – related violations
- Publication of sanctions
- Sanctions for senior managers and directors
- Fines

Core issue 3.5

Supervisory actions - impact on compliance

Impact can be demonstrated:

- Sectorial level (e.g. on the basis of off-site assessments supervisors observe risk decreasing trends: quantitative (e.g. number of clients from high risk countries) or qualitative (e.g. certain controls have been strengthened) data);
- Institutional level (subject person), real life examples (e.g. follow-up actions);
- On-site data (comprehensive supervisory findings; commonly identified breaches, etc.)

! Case examples/ aggregated supervisory data should be provided to support the conclusions (in addition to above data)

Core issue 3.6

Promoting a clear understanding of AML/CFT obligations and risks

- Level of compliance with R.34

Possible examples:

- Binding guidelines;
- Guidance notes;
- Trainings, seminars;
- Feedback (e.g. aggregated feedback on sectorial risks, annual reports, results of thematic reviews or strategic analyses; aggregated feedback on common deficiencies identified during on-site inspections);
- FIU feedback (typologies, etc.)
- Other forms of outreach (consultations);
- Meetings (e.g. annual/quarterly meetings with the key function holders (e.g. Board members, AMLCO, etc.);

Frequency and content of the trainings, seminars, consultations (topics discussed):



Council of Europe
Conseil de l'Europe
www.coe.int

MONEYVAL

Thank you!



Role of Associations in creating communication mechanisms in terms of Anti-Money Laundering and Countering Terrorist Financing (AML/CTF)

Compliance Risk and AML/CTF Committee (Association of Russian Banks)

Kazan, Sept 26-27, 2019



Association “Russia” – analytical and expert center of banking community

➤ Coordinates activity of Association members on the following issues:

- Evaluation of laws and regulations on countering illegal financial operations;
- Elaboration of approaches to legalization risk management;
- Application of international experience in terms of compliance risk management for the purposes of further developments aimed at application of such practices at the level of national AML/CTF system as well as in the area of risk management generally;
- Discussion and implementation of new approaches and initiatives aimed at cost saving for financial institutions while maintaining high level of compliance.

➤ Ensures effective interaction between Association members with:

- Representatives of the Central Bank, Rosfinmonitoring, other governmental agencies as well as civil organizations;
- Individuals with both Russian and international expertise;
- Financial Markets Association Council for Professional Qualifications Development



Coordination and interaction with Association “Russia” members:

- Direct interaction between the Association and financial institutions on outstanding issues in terms of current activity (question-answer);
- Polls for financial institutions for the purposes of public discussion of documents issued by the Central Bank as well as legislative acts, which should establish continuous dialogue with the regulators;
- **Operation of the Association’s Compliance Risk and AML/CTF Committee**



Compliance Risk and AML/CTF Committee

- Engagement of intellectual, managerial, and labor resources of Association members to solve pressing problems in terms of compliance risk management and AML/CTF;
- Elaboration of coordinated ideology and policy of Association members in terms of priority areas for the Committee's activity;
- Preparation of recommendations, standards, rules, and regulations on solving particular problems in these areas;
- Evaluation of draft laws and regulations for the purpose of their improvement, as well as amendment and updating of current laws of the Russian Federation.



Compliance Risk and AML/CTF Committee

Committee Chairman

Association: Vice-President, Committee Curator

**Group on International Standards
and Law**

AML/CTF Group

Group on working with information

**Group on New Compliance Risk
Management Techniques and
Instruments**



Compliance Risk and AML/CTF Committee's functions:

- Monitoring and analysis of current condition, problems, and trends in compliance risk management and AML/CTF;
- Study of bank and business communities' initiatives regarding compliance risk management and AML/CTF, their discussion with businessmen, and elaboration of implementation proposals;
- Study of international practices of compliance risk management and AML/CTF and elaboration of proposals on their implementation in Russia;
- Representation of the Association's stance in the Central Bank and other governmental agencies;
- Holding of conferences, roundtables, seminars, and other events.



Topics for AML/CTF meetings

2018

Private sector's engagement in national risk evaluation

Implementation of “client rehabilitation” mechanisms of financial institutions

New ML/FT trends, types, ways, and methods

Information interaction with Rosfinmonitoring

2019

Improvement of suspicious transaction reporting

Evaluation of legislative initiatives

Professional standards and requirements for employees of financial monitoring services



AML/CFT Committee goals for 2020

Engagement of private sector in national risk evaluation

Development of KYC procedures

Discussion of new ML/FT trends, types, ways, and methods

2020

Higher efficiency of information exchange with Rosfinmonitoring

Evaluation of legislative initiatives

Professional training of employees of financial monitoring services, higher financial awareness of the population

Interaction with international professional associations

Korea's Experience on Virtual Currencies

Kim JeeWoong
Korean Financial Intelligence Unit



Financial Services
Commission

Contents

I. Korean VC Market in 2017

II. Government Policy Actions

III. Plan to amend the AML/CFT Law

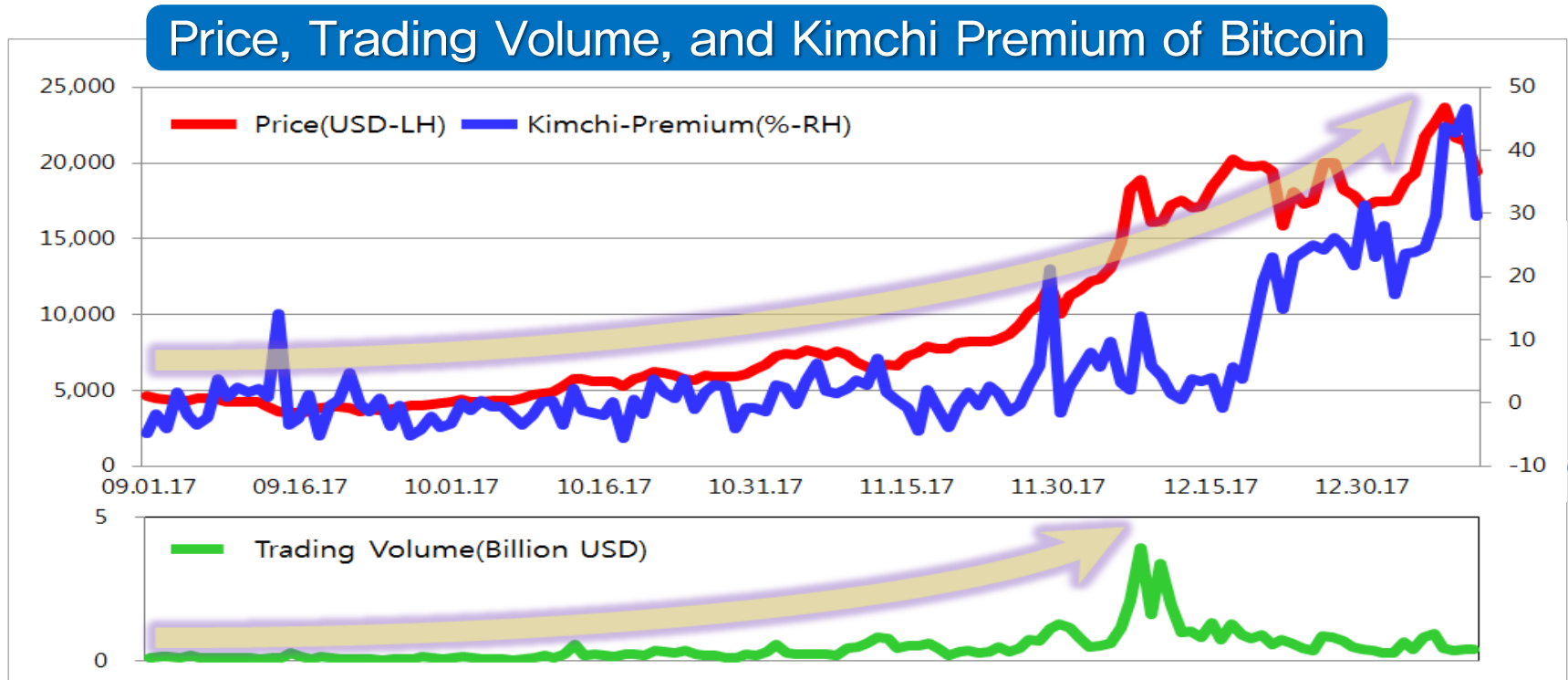
I. Korean VC Market in 2017

Korean VC Market in 2017

Overheated speculation on virtual currencies

- Price surged, trading volume skyrocketed
and the “Kimchi premium” widened

* Kimchi premium: The gap in virtual currency prices in Korean trading platforms compared to global trading platforms

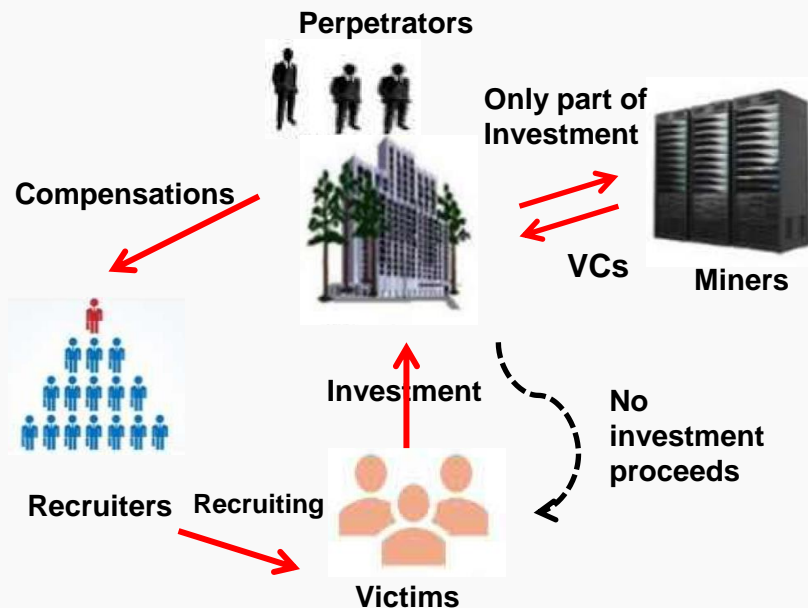


Korean VC Market in 2017

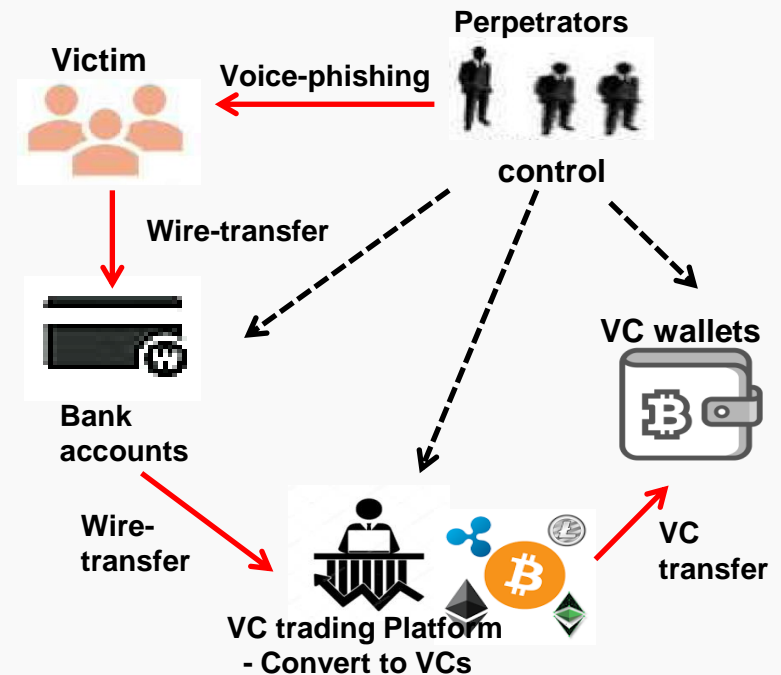
Widespread VC-related illegal activities

- Pyramid scheme, illegitimate fund-raising activities and money laundering of criminal proceeds

Pyramid Scheme



Money Laundering of Criminal Proceeds



II. Government Policy Actions

Government Measures in 2017

Joint task force
on virtual currencies



Counter measures

1

Crackdown on illegal activities related to virtual currencies by law enforcement agencies (Police Agency, Prosecutors' Office)

2

Protect trading platform users

- Inspections on violations of consumer protection articles (Fair Trade Commission)
- Inspections on IT systems security (Korea Communications Commission)

3

Issue a series of warnings on virtual currency investment and related transactions (Financial Services Commission, Financial Supervisory Service)

4

Impose ban on all kinds of ICOs (FSC, FSS)

5

Discuss measures to enable banks to identify trading platform users

- Introduced the real-name policy in virtual currency related transactions (FSC, FSS)
- Established guidelines on virtual currency

Measures of Financial Authorities in Jan 2018

1 Real-Name Policy in Virtual Currency Related transactions

- ✓ Users who want to make deposits at or withdrawals from virtual currency trading platforms must go through the real-name account service
- ✓ The service enables banks to better identify users

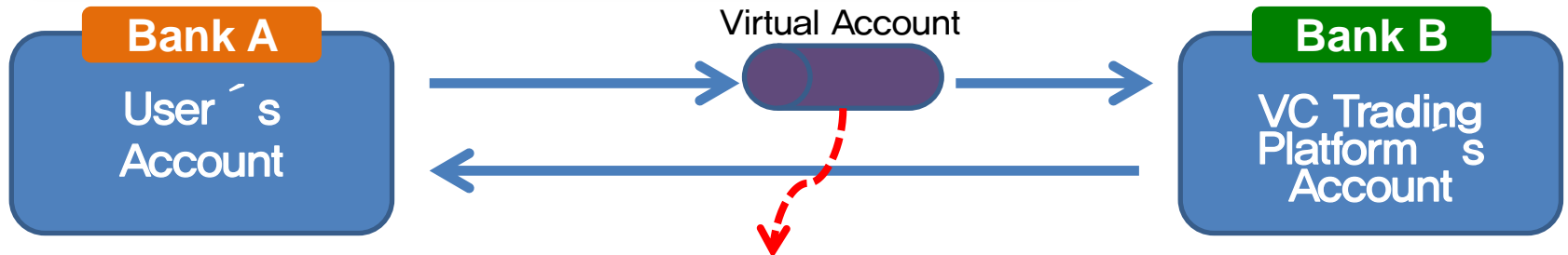
2 Virtual Currency AML Guidelines

- ✓ Roles and responsibilities of financial institutions including banks in order to effectively prevent money laundering while conducting virtual currency related activities



Real-Name Policy in VC Related Transactions

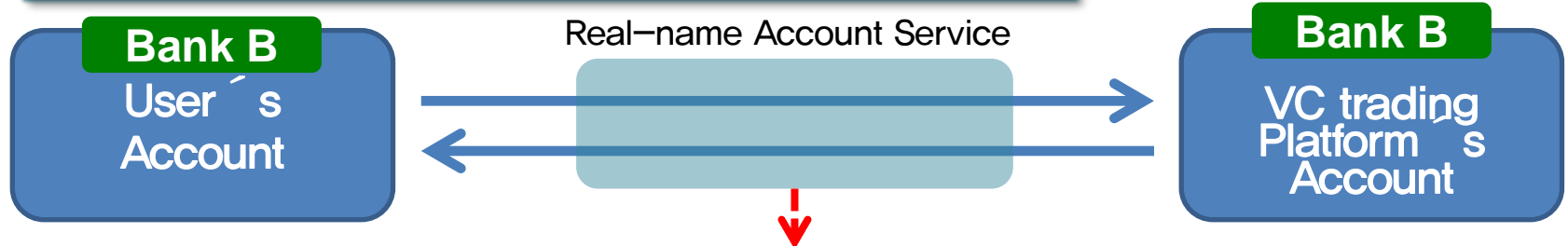
Before: Virtual Account Service



Virtual Account Service:

- Provided by **Bank B**, but controlled by **VC Trading Platform**
- **Bank B** could not identify who sent money to **VC Trading Platform**

After: Real-name Account Service



Real-name Account Service

- Provided by **Bank B**, and controlled by **Bank B**
- Users are required to have bank accounts of the same bank with **VC Trading Platform (Bank B)**
- **Bank B** can identify who sent money to **VC Trading Platform**

Virtual Currency AML Guidelines

KoFIU & FSS conducted joint on-site inspections on banks' compliance to AML/CFT obligations (Jan. 8 ~ Jan. 16)

The findings were reflected on the Guidelines

1

– Duty to identify VC trading platforms

– Conduct Enhanced Due Diligence on VC trading platforms

Whether or not VC trading platforms ①confirm the identification of users and ②manage users' deposits separately from assets of their own

2

Enhance monitoring(STR) on transactions belonging to the categories in the detailed list

3

Enhance internal control of financial institutions

– Explicitly specify the responsibilities of the board/executive management on virtual currency transactions

III. Plan to Amend AML/CFT Law

Plan to Amend the AML/CFT Law

1. AML Requirements for VC Trading Platforms

Duty to Register

Register with FIU

CDD

Conduct CDD for those entering into contract to perform transactions

STR

Transactions of virtual currency(including exchanges between VC and financial assets) are subjected to STR

Record Keeping

Retain CDD, STR, CTR records for 5 years

Internal Control

Establish internal control system to assess and manage ML risk for each virtual currency

Plan to Amend the AML/CFT Law

2. Additional Requirements for VC Trading Platforms

- A. Transaction records must be retained separately for each user
- B. Information security management system must be certified

3. When dealing with VC Trading Platforms, financial institutions must:

- A. Confirm whether or not the VC trading platform has:
 - ①registered with FIU and ②certified its information security management system
- B. Reject financial transactions for the following VC trading platforms
 - ①those which did not register with FIU and ②those which did not get their information security management system certified



***Thank you
entro21@korea.kr***



Financial Services
Commission



Public-Private Cooperation on Internet Finance Regulation



Key Points

1. Fast growth of Internet finance: benefits and challenges presented
2. National Internet Finance Association of China (NIFA) and its unique advantages
3. Joint efforts and initial achievements of PBC and NIFA
4. Future works

I. Fast growth of Internet finance: benefits and challenges presented

1. Improve accessibility, quality, and efficiency of financial services;
2. Increase difficulties of identity identification, transaction monitoring and ML crime confiscation;
3. For supervisors: priorities, coordination, RegTech application, forward-looking research, while limited resources....



II. National Internet Finance Association of China (NIFA) and its unique advantages

1. A strong team with both supervisory experience, academic expertise, and professional insights;
2. A wide coverage of Internet finance practitioners;
3. A firm hand on guiding, directing and urging all members.

III. Joint efforts and initial achievements of PBC and NIFA

1. Promulgation of a general law: *Administrative Measures for Internet Financial Institutions in Anti-money Laundering and Counter-terrorist Financing*
2. Preparation of industrial guidance;
3. Construction of a monitoring platform: *Online Monitoring Platform for Anti-money Laundering and Counter-terrorist Financing in the Internet Finance Industry.*



IV. Future works

1. Intensify cooperation with NIFA on Internet finance and other new technologies;
2. Explore cooperation with lawyers, accountants and so on for better ML supervision on DNFBPS.

THANK YOU!

AML/CFT Supervision of Commercial Banks in Kyrgyzstan. AML/CFT Cooperation.

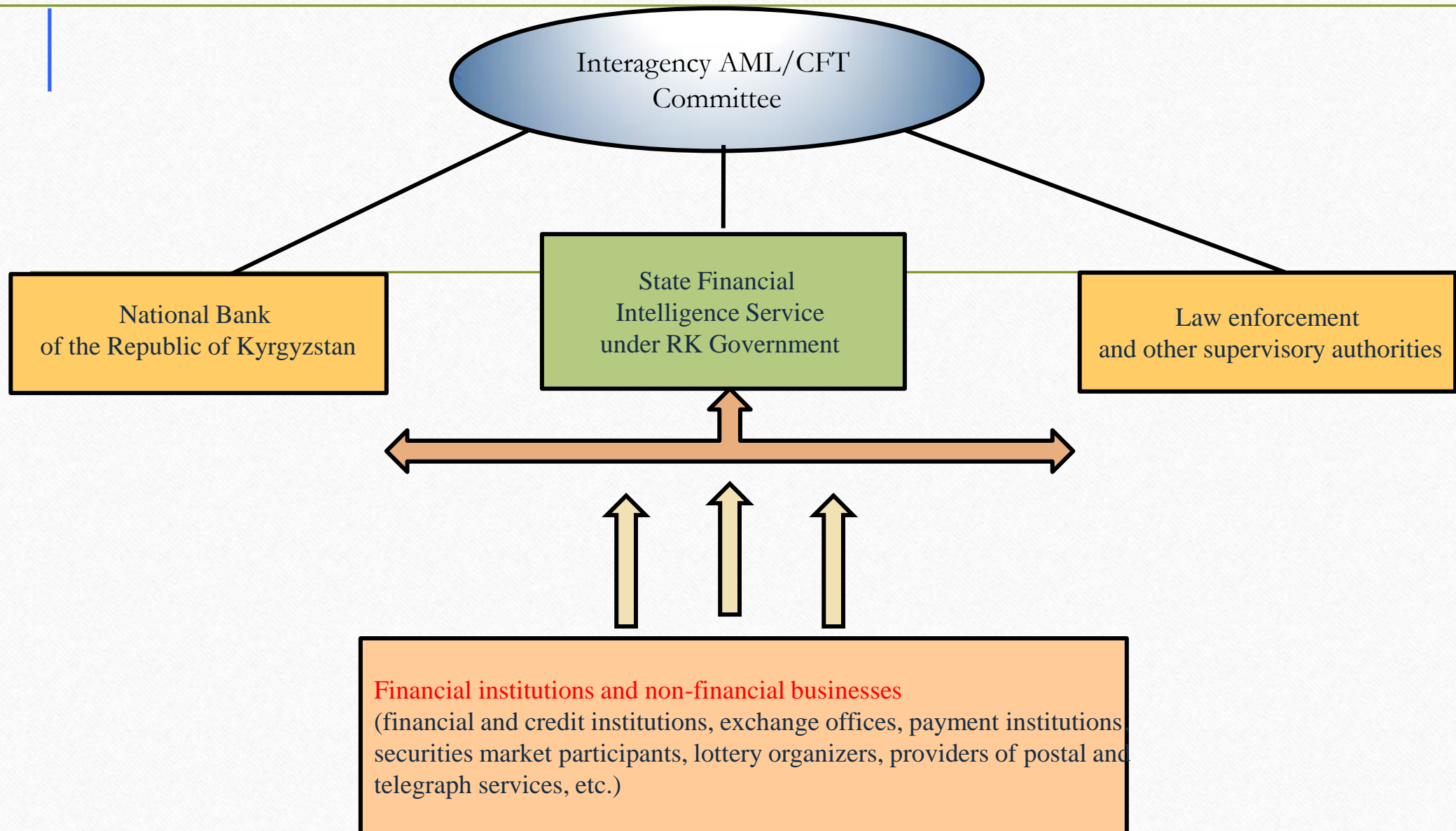
National Bank of the Republic of Kyrgyzstan

Directorate of Bank Supervision 1

Zhyldyz Imanbaeva, senior inspector

26-27 September 2019, Kazan, Russia

National AML/CFT System



Banks and Non-financial Credit Institutions as of September 4, 2019

Reporting entities	Total
Commercial banks	24
Microfinance organizations (microfinance and microcredit companies and microcredit agencies)	140
Credit unions and credit bureaus	101
Specialized financial and credit institutions (Financial Company of Credit Unions)	1
Exchange offices	410
Payment system operators and payment institutions	22

Kyrgyzstan's AML/CFT Law

Starting H1 2018, Kyrgyzstan's AML/CFT Law has been amended to bring it into line with the FATF Recommendations and to address the findings of the Mutual Evaluation of its AML/CFT system.

- RK Law "On Combating Money Laundering and the Financing of Terrorism" No. 87 of August 6, 2018;
- RK Government Resolution No. 606 dated December 25, 2018 "On measures to implement the RK Law 'On Combating Money Laundering and the Financing of Terrorism'" (re)establishing the AML/CFT Committee and adopting 13 regulations.

Regulations adopted by RK Government Resolution No. 606 dated December 25, 2018 "On measures to implement the RK Law 'On AML/CFT'" (13 regulations):

- 1) AML/CFT Committee Regulations;
- 2) Regulations on the Monitoring of Compliance with the RK AML/CFT Law;
- 3) Regulations on the Provision of Information and Documents to RK Financial Intelligence Unit;
- 4) Regulations on Cooperation between the RK Financial Intelligence Unit and Other Government Agencies;
- 5) Regulations on the Listings of Individuals, Entities, Groups and Organizations Known to Be Involved in Terrorism, Extremism, the Proliferation of Weapons of Mass Destruction and Money Laundering;

Regulations adopted by RK Government Resolution No. 606 dated December 25, 2018 "On measures to implement the RK Law 'On AML/CFT'" (13 regulations):

- 6) Regulations on the Suspension of Transactions, Freezing and Unfreezing of Transactions and (or) Funds, Provision of Access to Frozen Funds and Management Thereof;
- 7) Regulations on the Electronic Database of Beneficial Owners of Legal Persons;
- 8) Regulations on the Electronic Database of Declared Cash or Bearer Negotiable Instruments Transported Across the Customs Border of the Eurasian Economic Union into the Kyrgyz Republic;

Regulations adopted by RK Government Resolution No. 606 dated December 25, 2018 "On measures to implement the RK Law 'On AML/CFT' (13 regulations):

- 9) Regulations on the Application of Measures (Sanctions) against High-risk Countries;
- 10) Regulations on the General Requirements for an Internal Control Program;
- 11) Customer Due Diligence Regulations;
- 12) International Cooperation Regulations;
- 13) ML/TF Risk Assessment Regulations.

Changes in AML/CFT Legislation

Earlier version	Revised version
The term " risk-based approach " was not used; however, the main principles and approaches underlying it did exist.	Risk-based approach
Internal controls	Internal control program
Beneficial owner (beneficiary)	Beneficial owner
Foreign politically exposed persons	Public officials: <ul style="list-style-type: none"> - foreign public official; - domestic public official; - public official of an international organization
-	ML/TF risk assessment (national risk assessment → NRA report)
-	Measures to prevent the misuse of non-profit organizations

Changes in AML/CFT Legislation

Earlier version	Revised version
-	Measures to prevent the misuse of non-profit organizations
-	Measures to facilitate transparency of beneficial ownership <ul style="list-style-type: none">- Compiling by legal persons of beneficial ownership information- Maintaining by the FIU of an electronic database of beneficial ownership information
-	Electronic database of declared cash or bearer negotiable instruments transported across the customs border of the Eurasian Economic Union into the Kyrgyz Republic. This database is compiled and maintained by the State Customs Service under the RK Government, which provides the FIU with direct access to it.

Changes in AML/CFT Legislation

Earlier version	Revised version
<p><u>The term "CDD" was not used; however, FIs were required to conduct identification and verification procedures by the FATF Recommendations.</u></p>	<p>Customer due diligence</p>
<p><u>Identification of the customer and its beneficial owner involved in occasional transactions without opening a bank account:</u></p> <ul style="list-style-type: none"> - Equals to or above 1m som – full identification; - Less than 1m som – simplified customer identification (establishing the custom's identify using ID); - No identification was required for foreign currency exchange transactions under 50,000 som in cash. 	<ul style="list-style-type: none"> - Due diligence on customers and beneficial owners involved in occasional transactions without opening a bank account in the amount equal to or above 70,000 som – full identification; - With single or several interrelated foreign currency exchange transactions in the amount of 1 million som or more in cash– full identification; - With single or several interrelated foreign currency exchange transactions in the amont of 70,000 to 1 million som in cash – simplified identification (establishing the custom's identify using ID);

Changes in AML/CFT Legislation

Earlier version	Revised version
Transactions subject to mandatory controls: <ul style="list-style-type: none">- Transactions in the amount equal to or above 1m som;- Suspicious transactions as per the FIU's list	<u>Abolishment of the 1m som threshold for all transactions</u> Transactions subject to monitoring and reporting: <ul style="list-style-type: none">- suspicious transaction reports;- reports on transactions involving natural or legal persons from high-risk jurisdictions;- reports on transactions involving natural persons convicted of ML/TF offences;- reports on cash and non-cash transactions above the designated threshold. <p>*No threshold amount has been set as of now.</p>

Transactions Subject to Monitoring and Reporting

Report type	Transaction amount	Reporting deadline
Suspicious transactions report:	Irrespective of the transaction amount as per the list of suspicious transaction indicators (codes) adopted by the FIU.	within five (5) hours of the transaction being declared, in accordance with the established procedure, suspicious
Reports on transactions involving natural or legal persons from high-risk jurisdictions	Irrespective of the transaction amount	within two (2) business days of the transaction date
Reports on transactions involving natural persons convicted of ML/TF offences	Irrespective of the transaction amount	within two (2) business days of the transaction date
Cash/non-cash transaction reports	<p>In the amount equal to or above the designated threshold</p> <p>*The list of cash transactions and the applicable threshold amount are established by the RK Government based on the NRA findings.</p> <p><u>*No threshold amounts have been set as of now.</u></p>	<ul style="list-style-type: none"> - within two (3) business days of the transaction date - subject to FIU's request – within ten (10) business days of the request submission

Changes in AML/CFT Legislation

Earlier version	Revised version
The requirement to have an AML/CFTE certificate issued by an educational establishment upon succesful completion of an exam/test by a bank employee	<ul style="list-style-type: none">- Persons who have completed an AML/CFT training course offered by an educational establishment undergo final certification at the RK State Financial Intelligence Service's Training and Methodology Center;- SFIS notifies the educational establishment of the persons who have passed the final certification;- The educational establishment, in response to the information provided by SFIS, issues certificates of completion.

RK National Bank Board Resolution No. No. 2019-P-12\42-1-(NPA) dated August 14, 2019
amended and supplemented RK National Bank regulations (comes into force November 1, 2019):

- Regulations on the Minimum AML/CFT Internal Control Requirements for Commercial Banks;
- Guidance on dealing with bank (deposit) accounts(including KYC policies)
- RKNB Board Resolution "On the Requirements for Identifying Entities and Establishing a List of Offshore Jurisdictions";
- Regulations on Foreign Currency Exchange Transactions in Kyrgyzstan,
- etc.

New RKNB regulations for managing compliance and ML/TF risks

- Guidelines for setting up internal control and audit systems in banks and non-bank financial and credit institutions licensed and regulated by RKNB (adopted by RKNB Board Resolution No. 2017-P-12/25-3-(NPA) dated June 15, 2017, Section 4 "COMPLIANCE MONITORING SYSTEM"
- Regulations on the Minimum Risk Management Requirements for RK Banks (adopted by RKNB Board Resolution No. 2017-P-12/25-8-(NPA) dated June 15, 2017, Section 13 "COMPLIANCE RISK"

Compliance and ML/TF Risk Management

Risk-based Approach

- **"Risk"** means the likelihood that any anticipated or unforeseen events may have a negative impact on a bank's capital or revenue.
- **"Risk management system"** means a process consisting of four core elements: risk identification, risk measurement, risk control and risk monitoring.
- **"Compliance risk"** means the likelihood of losses resulting from non-compliance by a bank or its employees with legislative requirements, RKNB regulations and the bank's internal guidelines, incl. internal AML/CFT requirements, that govern the provision by the bank of services and execution of transactions in the financial market, as well as foreign legislative requirements that influence the bank's operations.
- **"ML/TEF risk"** means the risk of direct or indirect losses that a bank is exposed to as a result of its non-compliance with AML/CFT requirements, guidelines or standards due to the involvement of the bank, its customers and partners in ML/TEF.
- **"Risk appetite"** means the cumulative amount and types of risk that a bank is willing to take in order to meet its strategic objectives and implement a business plan, taking into account complex risks such as the bank's reputation and unethical practices. Risk appetite is taken into account when developing a bank's growth strategy and business plan.
- **"Bank's risk profile"** means a summary of all current types and levels of risks that reflect all underlying problems faced by a bank as well as conclusions based on the results of the current (last updated) assessment of the available information on these risks.

Compliance and ML/TF Risk Management Structure in Commercial Banks

Old structure (internal AML/CFT controls)

1 business unit of the AML/CFT Internal Control Service reporting to the Bank's Board of Directors

The Service was tasked with setting up AML/CFT internal controls

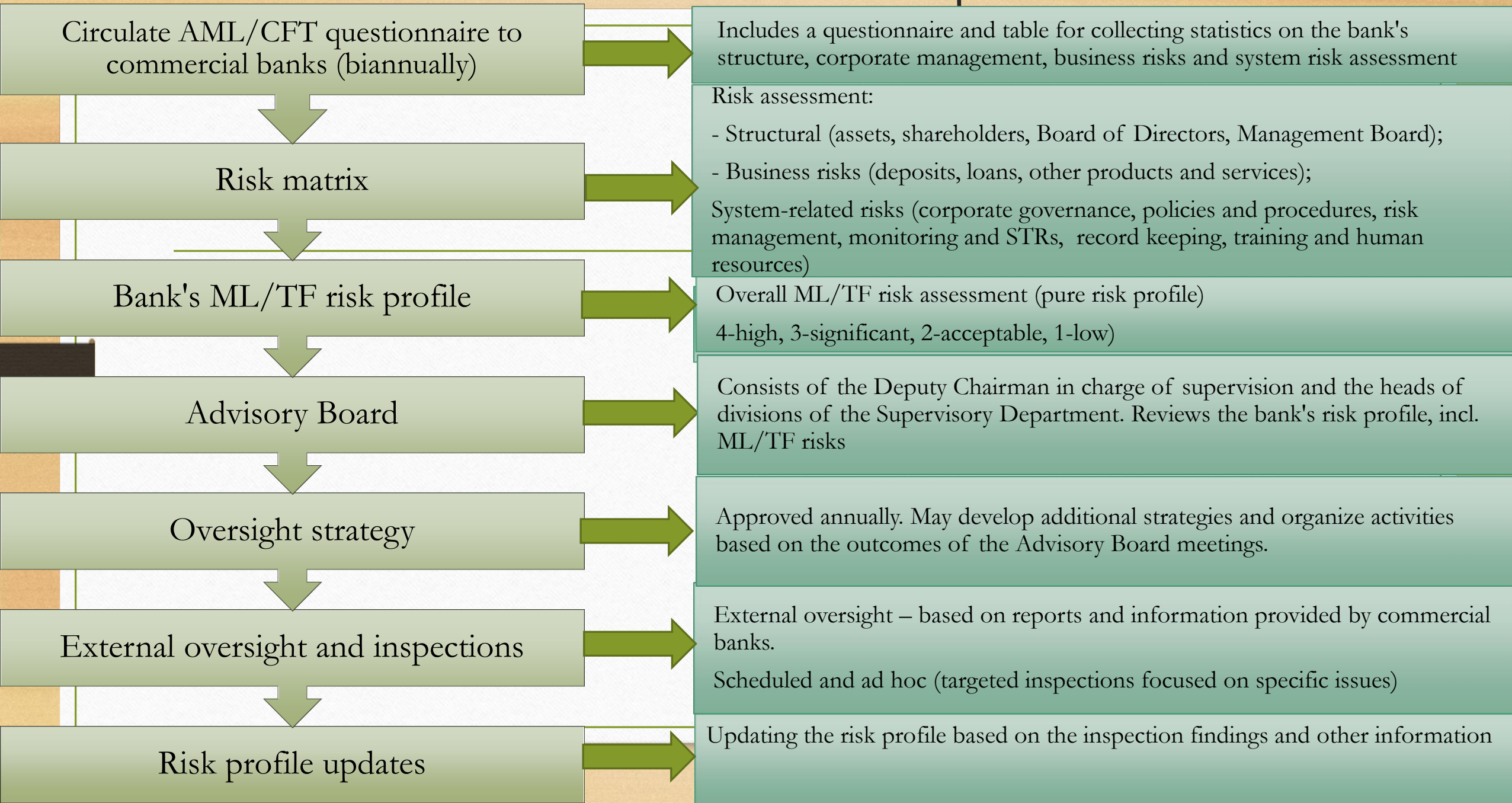
New structure (compliance controls + AML/CFT)

Compliance Control Service (reports to the Board of Directors) includes 2 business units:

- Compliance Office
- AML/CFT Office

- monitor and manage the bank's compliance risks;
- set up AML/CFT internal controls in the bank;
- monitor compliance of the bank's compliance risk management policies and procedures with legal requirements;
- monitor the bank's handling of customer complaints;
- identify, assess and monitor conflicts of interest;
- other functions.

RKNB's Risk-based Supervision



Enforcement Measures Used against Banks

- Remedial instruction
- Fine:
 - Subject to the decision of the RKNB Supervisory Committee (in the amount of not more than 10% of the mandated minimum amount of the authorized capital (600m som), i.e., not more than 60m som)
 - As per the Code of Violations (for offences covered by parts 1 and 2 of Article 216).
- Order
- Tightening of economic standards and requirements
- Restrictions or prohibitions (e.g., suspension of, or limits on, certain types of banking operations)
- Suspension or dismissal of officials, changes in governing bodies
- Introduction of a special regime
- License revocation

RK Code of Violations No. 58 of April 13, 2017

- **Article 18 Liability of legal persons**

A legal person who has committed a violation shall be held liable if a natural person with whom it maintains an employment relationship, or a natural person who performs certain acts for the benefit of such legal person under a contract, was aware or could and should have been aware of the wrongfulness of his act (act or omission).

- **Article 216 Violation of the anti-money laundering and combating the financing of terrorism/extremism requirements**

1. Violation of the anti-money laundering and combating the financing of terrorism/extremism requirements – is punishable by a category-4 fine (230 standard units* (23,000 som) for legal persons).
2. Violation of the requirements for the identification/verification of customers and identification of beneficial owners (beneficiaries) or monitoring the customer's financial activities – is punishable by a category-5 fine (280 standard units (28,000 som) for legal persons).
3. Violation of the procedure for reporting transactions subject to special control – is punishable by a category-7 fine (450 standard units (45,000 som) for legal persons).
4. Violation of the procedure for freezing funds and/or transactions – is punishable by a category-8 fine (550 standard units (55,000 som) for legal persons).

** 1 standard unit = 100 som*

Cooperation between the RK National Bank and the RK State Financial Intelligence Service

In accordance with a cooperation and information sharing agreement between the RK National Bank and the RK State Financial Intelligence Service of March 12, 2012, the parties shall:

- share information on the identified AML/CFT violations and shortcomings in the activities of banks and NFCIs:
 - Upon detection of non-compliance with AML/CFT requirements made in the course of a comprehensive (targeted) inspection, the RK National Bank shall, no later than 3 business days, submit a report on the detected violations;
 - Based on the results of a comprehensive (targeted) inspection, no later than 10 business days after the submission of a report to the bank/FCI, provide a summary of the identified violations and shortcomings in internal controls;
 - If there is a suspicion that the bank's/FCI's transactions are related to ML/TF, report them to the RK SFIS for a follow-up action (investigation).
- coordinate draft AML/CFT regulations and guidelines;
- organize training workshops and meetings, as well as participate in workshops via SFIS videoconferencing network;
- etc.

Cooperation between RKNB and commercial banks

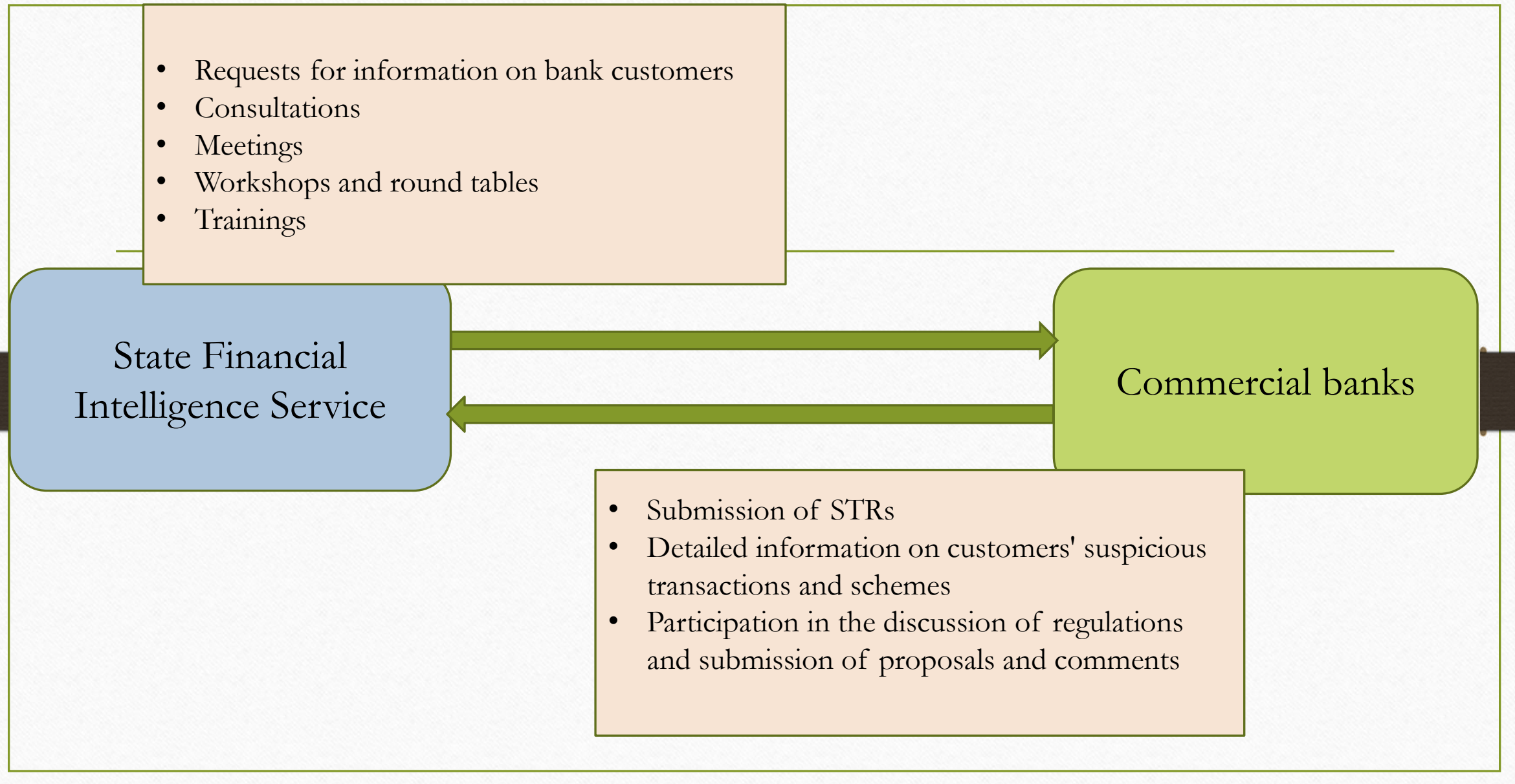
- AML/CFT questionnaire
- Requests for customer information
- Consultations
- Discussion of draft regulations
- Circulation of reports on risks and measures to mitigate them
- Dispatch of remedial instructions and warnings
- Meetings to discuss certain issues when necessary

National Bank

Commercial banks

- Statistics and responses to AML/CFT questionnaire
- Submission of customer information in response to RKNB's requests
- Submission of information on identified ML/TF and compliance risks
- Reporting on compliance with RKNB's remedial instructions and recommendations

Cooperation between SFIS and commercial banks



Cooperation between KIKIND and the Union of Kyrgyzstan's Banks

- Communication of banks' common position
- Participation in the discussion of regulations
- Organizing workshops and round tables
- AML/CFT trainings

National Bank

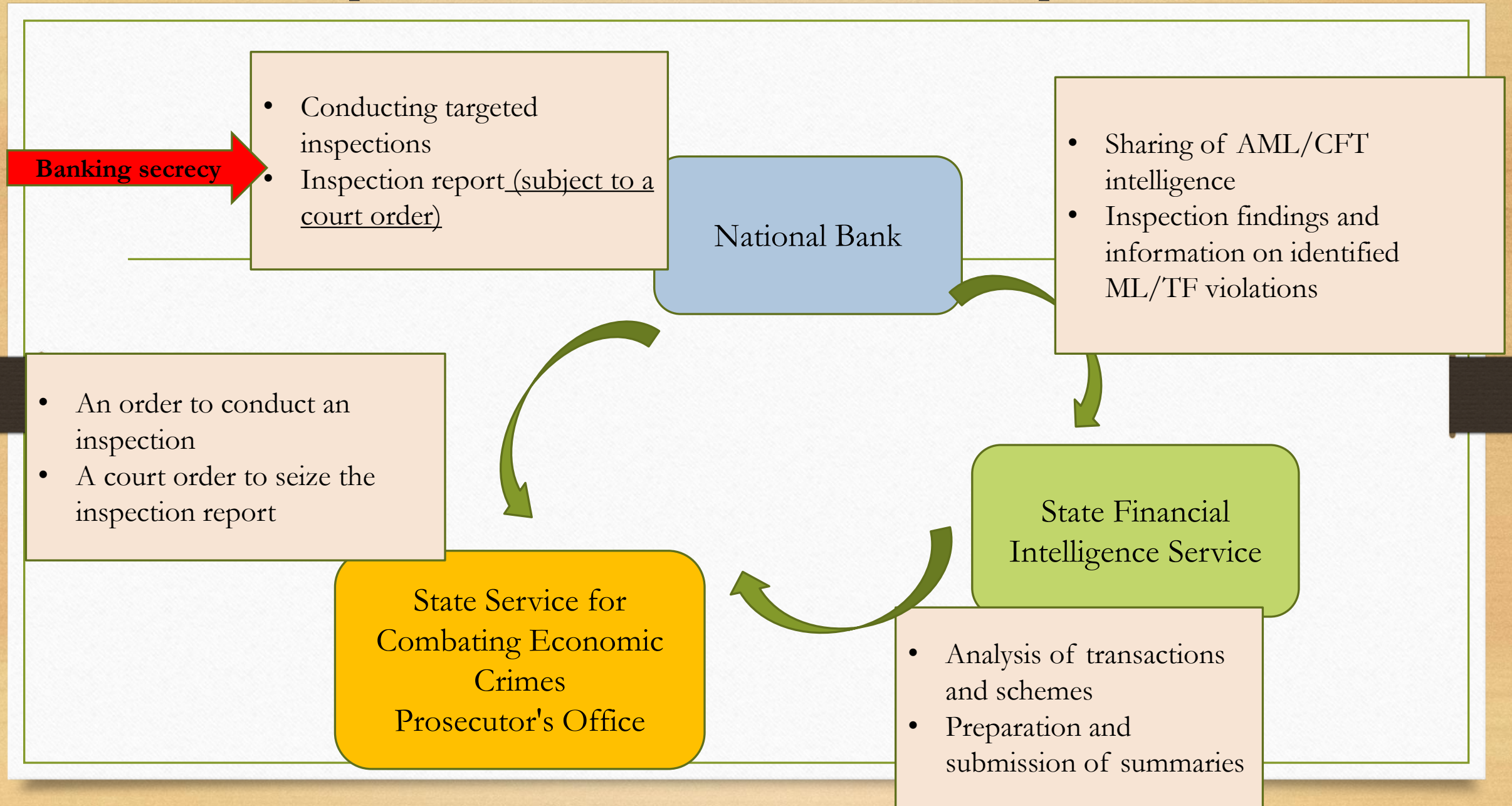
Union of Kyrgyzstan's Banks

AML/CFT consultations
Meetings of the heads of compliance units

Commercial banks

- Membership
- Pursuing common agenda
- Representing the private sector's interests
- Discussion of contentious issues
- Lobbying on behalf of the banking sector

Cooperation between RKNB and other supervisors



Cooperation between RKNB and foreign supervisors

- Concluded cooperation agreements, incl. on AML/CTF, with:

 - National Bank of the Russian Federation;
 - National Bank of Belarus;
 - National Bank of Ukraine;
 - National Bank of Cyprus;
 - People's Bank of China.
- Cooperation with foreign FIUs and other supervisors, incl. to request additional information, is conducted through the RK State Financial Intelligence Service.

Thank you

STR: country assessment experience, feedback mechanisms, key indicators of effectiveness





Core Issue 4.5.

- To what extent do financial institutions and DNFBPs meet their reporting obligations on the suspected proceeds of crime and funds in support of terrorism?

Examples of Specific Factors that could support the conclusions (Core Issue 4.5.)



- Do internal policies and controls of the financial institutions and groups, and DNFBPs enable timely review of: (i) complex or unusual transactions, (ii) potential STRs for reporting to the FIU, and (iii) potential false-positives? To what extent do the STRs reported contain complete, accurate and adequate information relating to the suspicious transaction?
- What measures are being taken to increase the effectiveness of the STR program?
- How well is feedback provided to assist financial institutions and DNFBPs in detecting and reporting suspicious transactions?

Suspicious transaction reporting

The main disadvantages of countries



- **Delays in informing and poor quality of STRs**
- **Sending messages only on the basis of «red flags», and not on the basis of suspicion**
- **A small number of messages from DNFBP**
- **Insufficient feedback from the FIU**

Suspicious transaction reporting


Best practice



- Identification and reporting of TF
- Public-Private Partnerships on increasing the efficiency of reporting suspicious transactions
- Live Data Exchange
- Quality feedback on sent messages
- Taking measures to reduce the number of messages sent "just in case, for show"

STR mode in countries



Country	Characteristics of the STR mode	Number of STRs
Spain 	<p>Before submitting a message, financial institutions fill out a special review including a structured analysis of potentially suspicious activities with all related transactions, parties involved in the transaction, a decision on whether to submit a STR. Such a system helps to eliminate “false positives” and protective reporting. The number of STRs is not as low as it might seem. The quality is confirmed by the high level of use of STR (about 40%) and specific cases of significant investigations.</p> <p>DNFBP. Notaries are required to upload all information about notarial acts to a centralized database, to which the FIU has access, and also independently send STRs.</p> <p>Forensic accountants who investigate cases of fraud do not send STRs at all, because they believe that fraud is not related to money laundering.</p>	≈ 3000

STR mode in countries



Belgium



DNFBPs, which are obliged to send messages about transactions based on established threshold values / criteria (in particular, casinos), often send only such “objective” messages and do not send messages based on an analysis of the suspiciousness of their operations. However, it seems that notaries, accountants and tax consultants take into account “subjective” factors when deciding on the direction of STR. At the same time, lawyers and diamond dealers practically do not send STRs. Such an approach can make it difficult to identify cases of money laundering and lead to the fact that some crimes go unpunished.

there is no data

Realtors rely almost entirely on “objective” factors when sending STRs (in accordance with Section 20 of the AML / CFT Law).

Italy



A significant increase in the number of STRs in banks, after checking the AML / CFT, was associated with the presence of an element of “defensive” reporting.

72000

With the exception of notaries (for whom special guidelines have been developed), STRs are sent by sectors of the DNFBP to a small extent. In relative terms, the work of notaries in the field of STR reflects the close interaction of the state and the private sector. 72% of STRs were sent within two months, and 6% more than seven months after the event. The appraisers positively noted an increase in the operational efficiency of the STR.

STR mode in countries



Portugal



The requirements for STRs filling are understandable to financial institutions, and their reporting corresponds to their level of risk. However, financial institutions indicate that there are difficulties in detecting suspicious transactions related to the financing of terrorism. Financial institutions ask for additional guidance (recommendations) in this area.

There is no data

Sweden





Most DNFBPs send very few STRs, despite being highly vulnerable in some sectors (such as trust and corporate service providers, lawyers, and real estate agents). This may indicate a low awareness of the risks they face. Supervisors recognize this problem and try to improve the level of reporting by focusing on the description of the suspicious actions of the client, as well as pointing out the requirements for sending STRs during inspections. For example, supervisors understand that real estate agents submit a small number of STRs and suspects that this is not due to lack of knowledge, but rather because they have a high level of expectation of a certain level of “evidence” before deciding whether to file STRs.

≈ 10000

Large banks, constantly interacting with the FIU, have the opportunity to obtain information that helps in their submission of STRs, they are generally satisfied with the level of information received from the FIU.



STR mode in countries



Country	Characteristics of the STR mode	Number of STRs
Singapore 	DNFBP representatives do not seem to understand that the purpose of STRs is to provide the authorities with information that could lead to the disclosure of criminal behavior. DNFBPs require guidance describing specific examples of submission of STRs.	≈ 28000
Hong Kong China 	Over 6 years there has been a 4-fold increase in the number of STRs, which, according to the evaluators, reflects an increase in awareness in the banking sector. Although the volume of defensive STRs is decreasing, it remains a problem. Financial institutions indicated that the feedback they receive from the FIU can be improved by providing information on the usefulness and quality of information supplemented by strategic analysis and typologies tailored to the needs of their particular sectors. The FIU provides quarterly reports on STR analysis, and also discusses STR issues within the framework of a special working group	≈ 86000

STR mode in countries



Country	Characteristics of the STR mode	Number of STRs
Malaysia 	<p>Assessment team noted that the reporting entities with which it met were not sufficiently aware of the extent of the obligation to report attempted transactions.</p> <p>Given the context and risk in Malaysia, FT-related STRs are low. Although legal obligations are comprehensive and generally accepted, there is a need for more focused guides (FT risk indicators and red flags) related to specific sectors.</p> <p>The almost complete absence of STRs from professional lawyers seems to reflect a lack of supervisory attention rather than legal obstacles.</p>	≈30000
Mexico 	<p>The level of reporting appears fairly uneven across institutions within some sectors. For instance, reports filed by the top five entities within each sector in 2016 constitute a large percentage of the total filed by the whole sector: banks (75 percent), brokerage firms (89 percent), and exchange centres (70 percent).</p> <p>In an effort to improve the quality of reports, the FIU has been providing detailed feedback to individual FIs as well as at the sectorial level.</p> <p>STR reporting by large firms is not always as prompt as it should be.</p>	≈120000

STR mode in countries



USA Approximately 11% of all SARs are filled on the same day that suspicious activity is detected. The average amount of time during the 30-day SAR submission window from the moment of identifying new suspicious activity for submission of ATS is 17 calendar days. 1 mln. 600

FinCEN has published its recommendations on trafficking in persons. The number of SARs related to human trafficking has increased 7 times over the year. This change reflects the ability of banks to set up their monitoring systems to better capture certain types of suspicious activity and manage risks.

The private sector is working well with the FBI to identify TF related transactions.

By law, financial institutions are required to immediately notify law enforcement authorities by telephone and file a timely SAR when they identify a situation involving a violation requiring immediate attention, regardless of any threshold.

STR mode in countries



GB



Banks have been given 30/60 days to conduct their own investigation before submitting the SAR, however there is a requirement to report issues requiring immediate attention to the FIU, and all have confirmed that they send the SAP as soon as they reach the threshold of suspicion.

440
000

The FIU, together with the oversight bodies, are taking measures to increase the effectiveness of the SAR regime. This includes industry reports, advertising campaigns, and industry events dedicated to SAR. The Flag It Up campaign of the Ministry of the Interior, which focuses on the legal and accounting sectors, has led to a marked increase in the number of downloads of the respective FIU guidelines for submission of SAR.

The number of SARs has increased as a result of interaction between the public and private sectors through JMLIT, as well as the work of a specialized group in the FIU.

Australia



Austrak combines the functions of the FIU and the regulator. A system has been introduced in which financial institutions have the opportunity to notify the FIU of the upcoming filing of STRs, as well as directly interact with law enforcement agencies regarding the relevance of STRs. Reporting organizations emphasized problems in detecting FT in the absence of specific information, and the adoption of effective measures to prevent them.

There is
no data

STR mode in countries



Canada



In identifying suspicious transactions, financial institutions rely on both **automated monitoring systems and qualified employees**.

Special sections of STRs describe the cause of suspicion. Evaluators positively noted the evolution of this element of STR from a basic summary to a very thorough and complex analysis of facts. STRs are usually filed in 30 days. At the end of the internal assessment process, if no STR is filed, a record is made with the rationale for not reporting.

≈ 92000

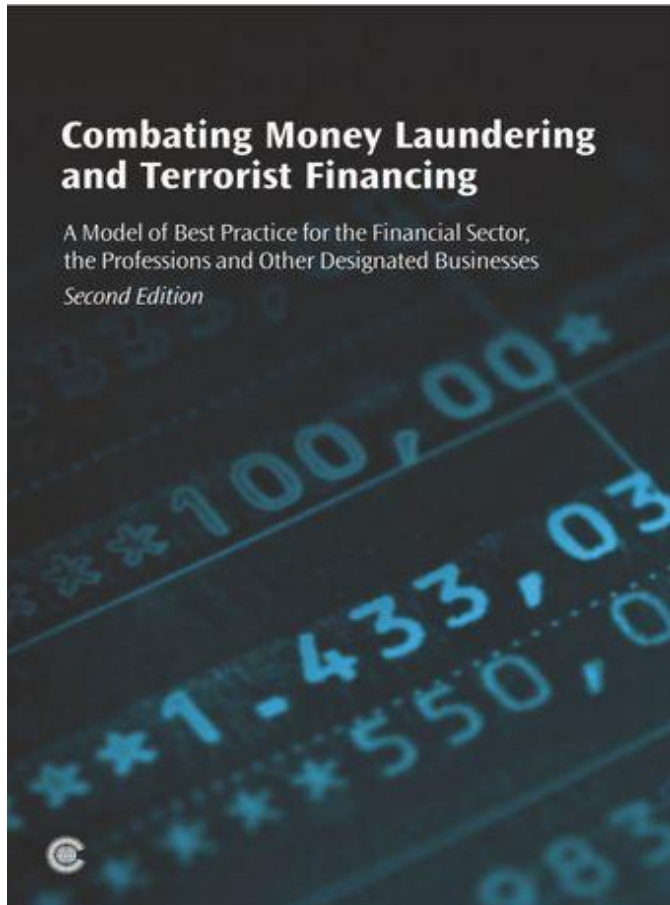
DNFBP Large casinos detect suspicious transactions not only through front-office employees, but also through **analytical monitoring tools developed at the corporate level**, as well as through video investigations to identify possible unusual customer actions.

The fact that accountants and notaries do not file STRs, and the number of STRs coming from the real estate sector is small, is worrisome.

In a number of sectors, the number of STRs filed has increased significantly, mainly as a result of outreach activities by FINTRAC.

Large financial institutions have good channels of communication with FINTRAC and they receive adequate reviews on an annual basis about the quality of their STRs and the number of convicted persons in cases initiated by FINTRAC. A special unit has been created at FINTRAK to provide feedback to financial institutions.

FATF Guidelines: Providing Feedback to Reporting Institutions and Other Persons



- It is recognised that measures to counter money laundering will be more effective if government ministries and agencies work in partnership with the financial sector.

- In relation to the reporting of suspicious transactions, an important element of this partnership approach is the need to provide feedback to institutions or persons which report suspicious transactions

Why is Feedback on Suspicious Transaction Reports Needed?



- ✓ It enables reporting institutions **to better educate their staff** as to the transactions which are suspicious and which should be reported. This leads staff to **make higher quality reports** which are more likely to correctly identify transactions connected with criminal activity;
- ✓ It provides compliance officers of reporting institutions with important information and results, allowing them to better perform that part of their function which requires them **to filter out reports made by staff which are not truly suspicious**. The correct identification of transactions connected with ML or other types of crime allows a more efficient use of the resources of both the financial intelligence unit and the reporting institution
- ✓ It also allows the institution to take appropriate action, for example **to close the customer's account** if he is convicted of an offence, or **to clear his name** if an investigation shows that there is nothing suspicious
- ✓ It can lead to improved reporting and investigative procedures, and is often of benefit to the supervisory authorities which regulate the reporting institutions;
- ✓ Feedback is one of the ways in which government and law enforcement can contribute to the partnership with the financial sector, and it provides information which demonstrates to the financial sector that the resources and effort committed by them to reporting suspicious transactions are worthwhile and that results are obtained

Types of Feedback



- statistics on the number of disclosures, with appropriate breakdowns, and on the results of the disclosures;
- information on current techniques, methods and trends (sometimes called «typologies»);
- sanitised examples of actual money laundering cases



- Number of STRs for the period (total and by sector or institution, volume of STRs, geographic areas from which STRs were transferred, types of transactions for which STRs are sent).
- Information on the number of open investigations, the number of closed cases, as well as cases referred to the prosecution authorities (breakdown by types of crimes committed and the amount of money, as well as the citizenship of the parties involved and which of the three stages of ML took place)

Other Information Which Could Be Provided



- An explanation of why ML takes place, a description of the ML process and the three stages of ML, including practical examples;
- An explanation of the legal obligation to report, to whom it applies and the sanctions (if any) for failing to report;
- The procedures and processes by which reports are made, analysed and investigated, and by which feedback is provided, allow FIUs to provide information on matters such as the length of time it can take for a criminal proceeding to be finalised or to explain that even though not every report results in a prosecution for ML, the report could be used as evidence or intelligence which contributes to a prosecution for a criminal offence, or provides other valuable intelligence information
- A summary of any legislative changes which may have been recently made in relation to the reporting regime or ML offences

Feedback methods



- written feedback (annual reports and regular newsletters)
- through personal meetings with financial institutions, including for a particular institution or its personnel, or for a wider range of institutions.
- training video courses
- electronic information systems, (information from websites, from other electronic databases or electronic message systems)



United Kingdom Financial Intelligence Unit (UKFIU)



A United Kingdom Financial Intelligence Unit (UKFIU) publication aimed at all stakeholders in the Suspicious Activity Reports (SARs) regime

What is SAR?

- this is information that warns law enforcement agencies that the client or his activities are suspicious, which may indicate his relationship with ML or TF.

The role of the FIU

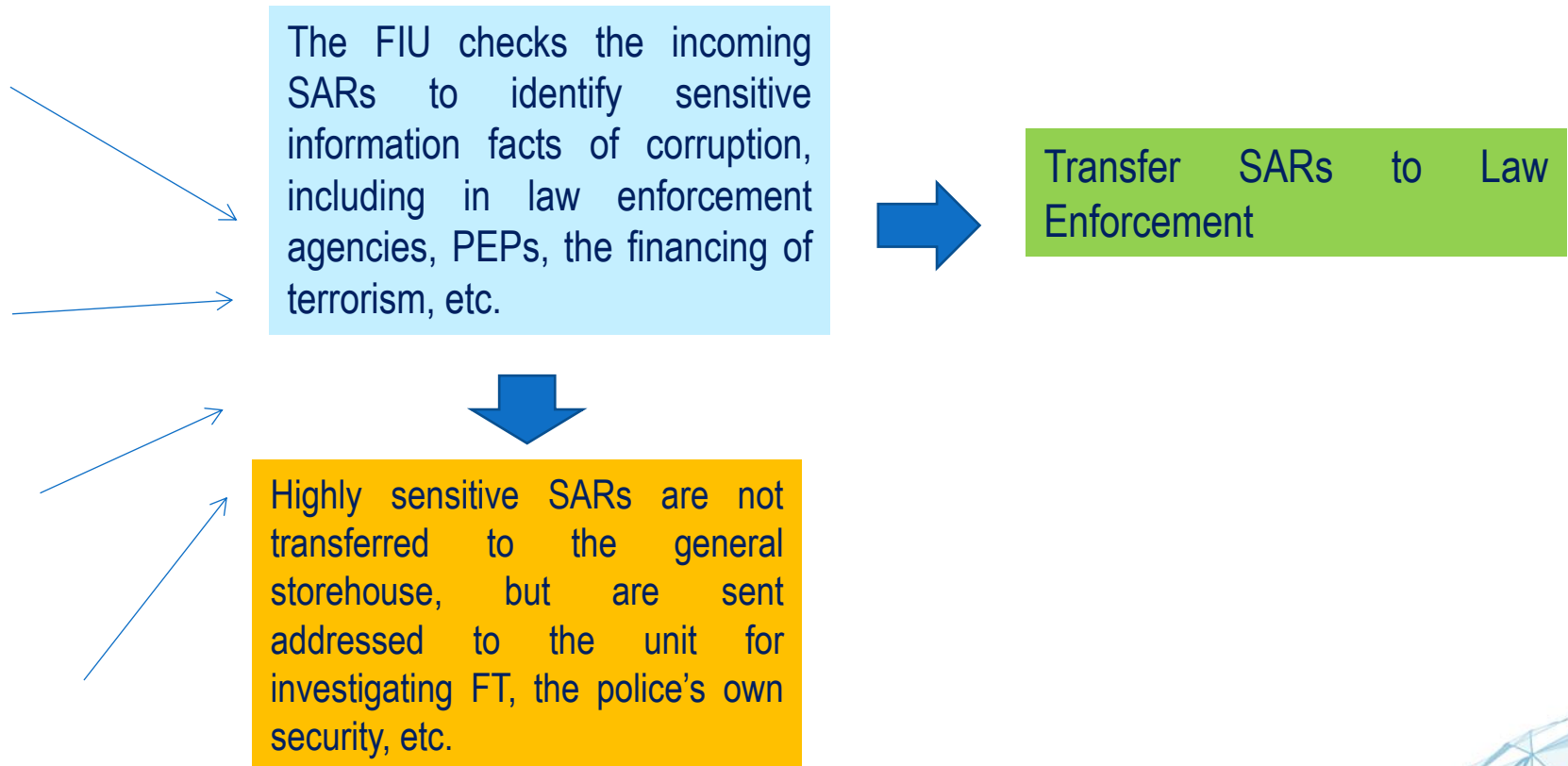
The FIU is responsible for obtaining, analyzing, conducting a financial investigation based on the received SARs

How to send SAR?

The easiest way to submit an SAR is through the secure SAR Online system, a free service providing instant acknowledgment of SAR acceptance. Reports can be sent 24/7. SAR Online can be accessed from the NCA homepage -www.nationalcrimeagency.gov.uk

United Kingdom Financial Intelligence Unit (UKFIU)

Distributed SARs Analysis Model





United Kingdom Financial Intelligence Unit (UKFIU)



Suspicious Activity Reports (SARs) Annual Report 2018

Statement by the Director of the National Agency for Combating Crime on the priority issue of improving the effectiveness of SPD

Detailed statistics of targeted SARs (by sector)

Activities conducted by the FIU in conjunction with supervisory authorities to increase the effectiveness of reporting suspicious transactions

General statistics on the use of SARs indicating the effectiveness of financial investigations

Case studies of the usefulness of SARs for investigations



United Kingdom Financial Intelligence Unit (UKFIU)



Guidance on submitting better quality Suspicious Activity Reports (SARs)

This is a United Kingdom Financial Intelligence Unit (UKFIU) product. It is aimed at all reporters of SARs and is produced in line with the National Crime Agency's commitment to share perspectives on the SARs regime.

May 2019

V3.0



SARs Reporter Booklet

July 2019

This is a UK Financial Intelligence Unit (UKFIU) product for reporters of Suspicious Activity Reports, produced in line with the National Crime Agency's commitment to share perspectives on the SARs regime.

Feedback mechanisms for sent STRs in Russia



Targeted interaction with financial institutions:

- sending thank you letters for the information that was used in conducting financial investigations.
- quarterly referral to the largest financial institutions of the results of the analysis of their STRs.

Compliance Council as a Feedback Mechanism



Федеральная служба
по финансовому мониторингу

Поиск по сайту



О Росфинмониторинге Деятельность Гражданам Организациям Государственная служба Контакты Пресс-служба

Главная / Деятельность / Надзорная деятельность / Совет Комплаенс

Совет Комплаенс

Что такое Совет комплаенс?

Совет комплаенс это консультативный орган при Межведомственной комиссии по противодействию легализации (отмыванию) доходов, полученных преступным путем, финансированию терроризма и финансированию распространения оружия массового уничтожения (в соответствии с Положением о Совете комплаенс от 06.07.2016 года).

Основная цель создания данного консультативного органа - формирование эффективной «обратной связи» с частным сектором по вопросам информационного обмена.

Аналогичные проекты реализуются и в других странах. Так, Австралийское подразделение финансовой разведки Аустрак (Australian Transaction Reports and Analysis Centre) реализует проект оперативного взаимодействия с банками Финтел Альянс (Fintel Alliance), включающий помимо банков и систем перевода денег Western Union и Pay Pal также федеральную полицию и налоговую службу. Помимо оперативной составляющей Финтел Альянс работает над инновациями в сфере ПОД/ФТ и управления рисками новых финансовых технологий (блокчейн, криптовалюты).

В Великобритании реализуется аналогичный, но с большим акцентом на правоохранительную составляющую проект Джимлет (JMLIT), организованный по инициативе Национального криминального агентства объединяющий представителей крупнейших банков, Британской банковской ассоциации, регулятивных органов, а также представителей научного сообщества. Работа Джимлет основана на модели экспертных групп, каждая из которых работает по определенной тематике, например, по борьбе с коррупцией. Банкам-участникам предоставляется расширенный доступ к информации, аккумулируемой финразведкой, при этом участники несут обязательства по неразглашению конфиденциальных сведений.

В настоящее время Совет комплаенс объединяет представителей крупнейших финансовых институтов и так называемых установленных нефинансовых предприятий и профессий. Помимо обмена информацией о новых рисках, выработке критериев о подозрительных операциях Совет комплаенс занимается вопросами совершенствования СПО, информационного обмена. Такого рода адресное взаимодействие с организациями, которые по сути генерируют основной объем информации позволяет влиять на параметры качества информационного потока.

Одним из приоритетных направлений деятельности Совета комплаенс является разработка критериев и моделей финансового поведения преступников в целях повышения эффективности и оперативности выявления операций, сопряженных с соответствующими рисками (в соответствии с Концепцией работы Совета комплаенс).

Стратегическая
цель:

Повышение качества СПО на основе риск-ориентированного подхода

Надзорная деятельность

Результаты проверок

Результаты анализа и обобщения
правоприменительной практики
контрольно-надзорной деятельности

Совет Комплаенс

Взаимодействие и координация

Международное сотрудничество

Государственные закупки

Информационные системы

Административные регламенты

Показатели деятельности и отчеты об их
исполнении

Результаты проверок

Использование бюджетных средств

Федеральные целевые и государственные
программы

Годовые отчеты

Государственные услуги

Сведения о признании судом
недействующими нормативных правовых
актов Росфинмониторинга

Судебный и административный порядок
обжалования нормативных правовых актов,
решений, действий (бездействия)
Росфинмониторинга, его территориальных
органов и их должностных лиц

В режиме видеоконференцсвязи принимают участие региональные советы, созданные на площадках Межрегиональных управлений. В общей сложности Совет объединяет более 100 участников – ведущих экспертов руководителей подразделений внутреннего контроля организаций.



Лн Ольга Хен-Дюновна (Нижегород),
Начальник отдела финансового мониторинга, ПАО
«НБД-Банк»

«Считаем создание Совета комплаенс, как консультативного экспертного органа, важным мероприятием, благодаря которому мы получили полезную площадку с широким и представительным кругом участников для обсуждения актуальных вопросов в области ПОД/ФТ, имеем возможность ознакомиться с передовыми практиками организации системы

внутреннего контроля в финансовых организациях....»



Лопатко Андрей Борисович (Москва)
Первый вице-президент
Начальник Управления финансового
мониторинга АО ЮниКредит Банк

“Создание Совета Комплаенс в нашей сфере можно сравнить с долгожданной встречей “живую” людей после длительного общения “по переписке”. Гораздо эффективнее, быстрее и понятнее можно доносить и обсуждать взаимные вопросы, вместе работать над повышением эффективности системы ПОД/ФТ. На данной площадке собрались специалисты не только из финансовой, но и из телекоммуникационной и других отраслей, что позволяет создавать максимально продуманные и реалистичные решения, учитывающие коллективный опыт и точку зрения...”



Марасеева Наталья Владимировна (Москва)
Руководитель Службы риск-менеджмент и комплаенс
ПАО «ТрансФин-М», член Правления

«Совет комплаенс предоставляет уникальные возможности коммуникаций с российскими и зарубежными экспертами в сфере ПОД/ФТ. Обмен опытом и лучшими практиками позволяет нам внедрять новые эффективные подходы в комплаенс нашей компании....»

Feedback mechanisms for sent STRs in Russia



- Using personal account on the Rosfinmonitoring website
 - Providing ML / FT typologies and sectoral risk assessments to all AML / CFT entities and supervisory authorities.
 - Providing analytical reports on the results of sending STRs to a specific sector and problematic issues of communication.
 - Providing the quality index of the information flow.

Personal Account on the Rosfinmonitoring website

Information Quality Index





Банк России

**TOPICAL ISSUES OF BUSINESS
REHABILITATION IN SITUATIONS WHERE
FINANCIAL INSTITUTIONS REFUSE TO
PERFORM THE TRANSACTION OR ENTER
INTO A BANK ACCOUNT (DEPOSIT)
AGREEMENT**

2019





Federal Law No. 115-FZ: a tool for combating suspicious transactions



refusal to perform the transaction



refusal to enter into a bank account (deposit) agreement



decision to terminate the bank account (deposit) agreement

Goals behind the Decision to Establish an Interagency Committee



- to enable an out-of-court defense of customer rights



- to enable a thorough and full review of the circumstances set forth in the customer's complaint



- to reduce tension associated with the application of AML measures

Cooperation with the Credit Institution to Facilitate Rehabilitation



1. Verify the nature of the CI's restrictive measures



2. Contact the CI for clarification of the reasons for refusal (where necessary)



3. Submit to the CI documents and/or information in support of arguments against the refusal



4. Receive from the CI a notification of the elimination of the grounds for refusal or impossibility of their elimination



5. Upon being notified of the impossibility of elimination of the grounds for refusal, file a complaint with the Bank of Russia's Interagency Committee

Interagency Committee's Operating Procedure



Cooperation with the Interagency Committee



Grounds for the Interagency Committee's refusal to consider the complaint



Adoption of the decision by the Interagency Committee and notification of the claimant and the financial institution

- in case of a positive decision

- in case of a negative decision

AML/CFT and Customer Rehabilitation: Guidance and Practical Tips for Entrepreneurs:

The working group, comprising representatives of the Bank of Russia, the Chamber of Commerce and Industry, public associations “Business Russia” and “OPORA RUSSIA”, and the Agency for Strategic Initiatives, has developed guidelines for entrepreneurs wishing to understand the reasons behind credit institutions' decision, made in accordance with the AML/CFT law, to refuse a request to perform transactions and enter into a bank account (deposit) agreement.





Банк России

THANK YOU

**E V. Leshcheva,
Head of the Directorate of Financial
Monitoring and Currency Control, Volgo-
Vyatka Main Directorate, Bank of Russia**

**Contact
details**

**tel.: 8 (831) 438-18-60
с 9:00 до 18:00 (MSK)**

E-mail

22gupost@cbr.ru

Bank of Russia Volgo-Vyatka Main Directorate
2019



**Financial monitoring Department under the
National Bank of Tajikistan**

Obligations of reporting entities under Order 129 for freezing and unfreezing assets of natural persons and legal entities included in lists related to terrorism

Appoint officer in charge and substitute officer for an absence period

While taking measures of KYC check the natural persons and legal entities on the presence in the lists

Freeze assets of persons included in lists of terrorists

Reporting entities are obliged:



Financial monitoring
Department



Reporting entities



State Committee on
National Security

List of Republic of Tajikistan consist of:



United list



International list



National list



Департаменти мониторинги молиявии
назди Бонки миллии Тоҷикистон



Financial Monitoring Department
under the National bank of Tajikistan



INFORMATION PAGE OF THE DEPARTMENT OF FINANCIAL MONITORING UNDER THE NATIONAL BANK OF TAJIKISTAN

Contents

[Home page](#)

[Laws and acts](#)

[FATF recommendations and
international regulations](#)

[Consultation of FATF](#)

[Guiding principles of UN Security
Council resolutions for private sector](#)

[Communication on legislative acts,
international standards and principles to
financial institutions and DNFBP](#)

[The list of terrorists and extremists](#)

[Typological research](#)

[Annual report:](#)

[for 2010-2011](#)

[for 2012](#)

[for 2013](#)

News



19.08.2019 **List established under UNSC resolution was changed**

Committee established pursuant to the UN Security Council resolutions 1267/1989/2253 approved changes to the list of individuals and entities associated with ISIL & AL-QAIDA.

01.08.2019

18.07.2019 **List established under UNSC resolution was amended**

Committee established pursuant to the UN Security Council resolutions 2374 approved amendments to the list of individuals and entities associated with Mali.

22.05.2019 **List established under UNSC resolution was changed**

Committee established pursuant to the UN Security Council resolutions 1267/1989/2253 approved changes to the list of individuals and entities associated with ISIL & AL-QAIDA.

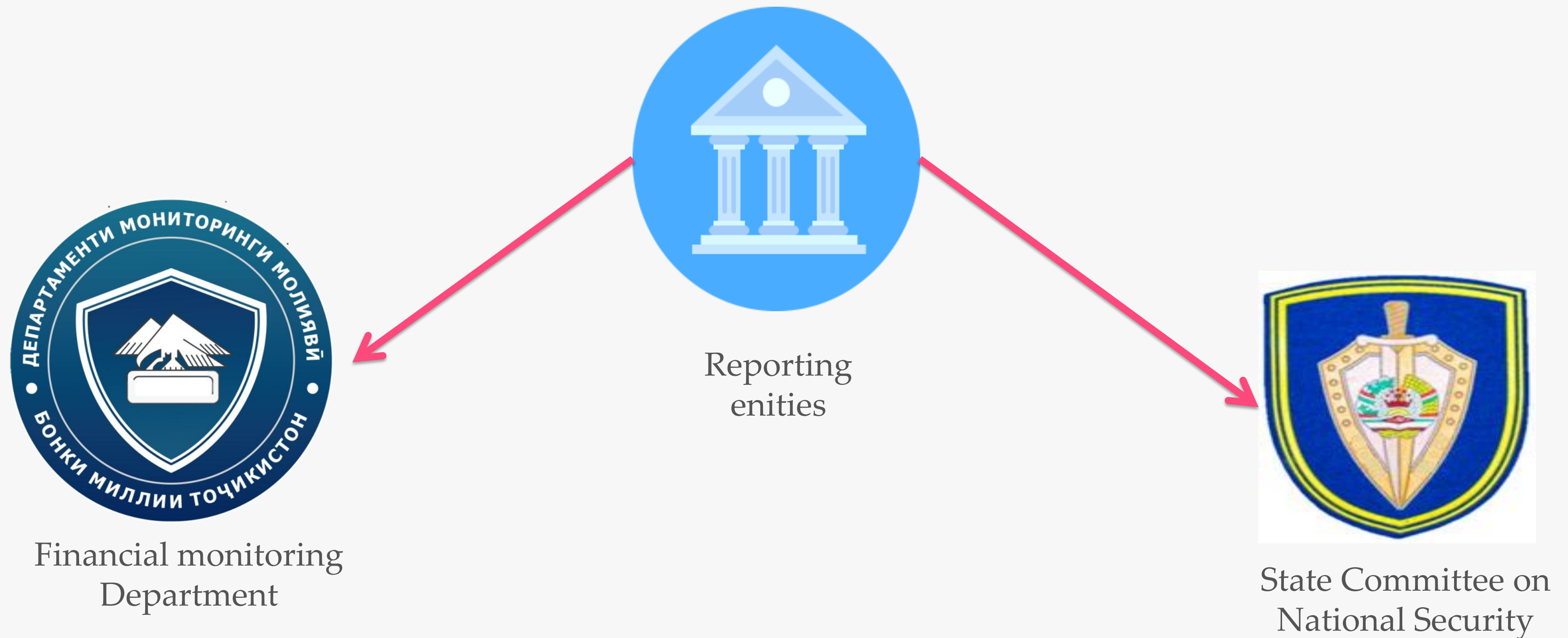
08.05.2019

[All news](#)

Address: Republic of Tajikistan, 734003,
Dushanbe, 107 A Rudaki avenue.

Contacts information: tel: +992(44) 600 36 84;
fax: +992(44) 600 36 87; e-mail: dmm@nbt.tj

Freezing of assets of terrorists in the Republic of Tajikistan



Reporting entities which do not adequately or fully follow-up to the regulations of the Order No.129 are liable under the legislation of the Republic of Tajikistan
(Item 59 of the Order No.129).



Mutual Freezing with Russian Federation



**Financial
monitoring
Department**

Exchange of
National Lists

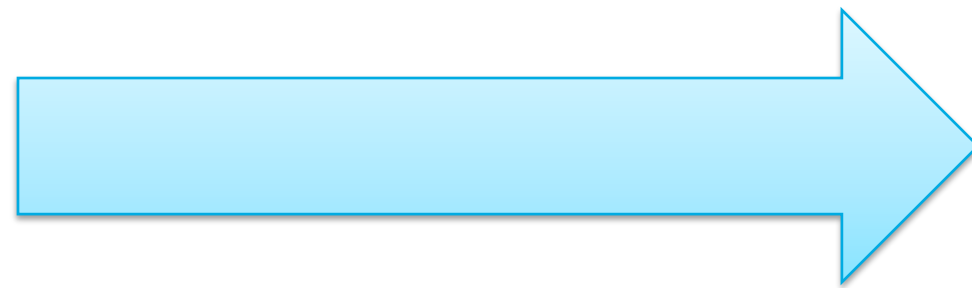


**Federal financial
monitoring
Service**

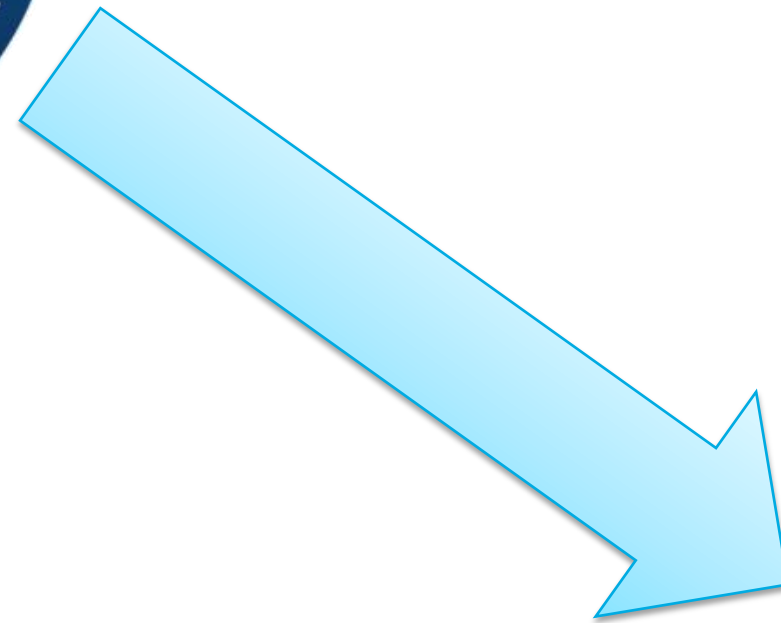
Mutual Freezing with Russian Federation



**Financial
monitoring
Department**



Decision
on freezing assets of persons of
National List of Russian Federation



Sending relevant inquiry to
reporting entities

Mutual Freezing with Russian Federation



Interagency commission on combating terrorism financing made a decision to freeze assets of persons from National List of the Republic of Tajikistan

As a result in Russian Federation were frozen 240 bank accounts of 163 persons from National List of the Republic of Tajikistan

Thanks for your
attention!



**PROFILING OF CRYPTOCURRENCY ECOSYSTEM
ACTORS FOR THE PURPOSE OF THE RISK
ASSESSMENT OF CRIMINAL BEHAVIOUR.
RISKS TO CRYPTOCURRENCY PROVIDERS AND
THE TRADITIONAL PRIVATE SECTOR AND
MONITORING METHODS.**

I

September 2019



Current Risks

01

Drug trafficking financing

02

The risk of transferring foreign economic activity into the underground in order to avoid taxes payment and customs duties

03

Withdrawal of funds abroad in order to legalize the proceeds of crime

04

“Multiplier” of the illicit cash flow





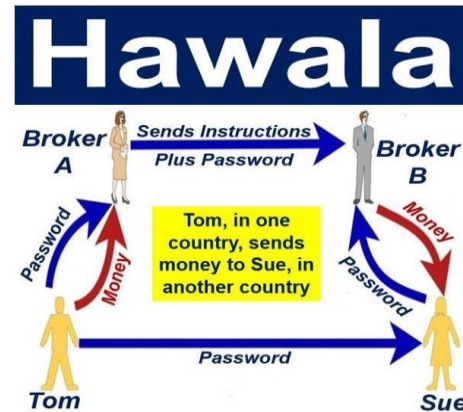
Possible risks in the nearest future

01 | The increase of existing threats and the emergence of new one in the financial sphere due to the emerging new technologies of financial instruments traded

02 | Hawala – Hi-tech

03 | Significant counterproductive impact on national economies due to the increased capitalization and the number of cryptocurrencies

04 | Cryptocurrency conversion of retail aggregators and marketplaces





Main vulnerabilities



The lack of control over AML regulators at the platforms for exchanging cryptocurrency for Fiat and cryptocurrencies among themselves.



The lack of control over regular private exchange of cash for cryptocurrencies



The lack of accounting of cryptocurrencies as a means of financing foreign economic activity and control of these financial flows





Sources of information for profiling



Internet: Internet publications, information disclosure by participants in cryptocurrency activities, corporate websites, private sector



Official documents on registering and obtaining licenses in the official bodies of activities registration of different jurisdictions



Transaction nature at the addresses controlled by a subject of cryptocurrency activities, the analysis of counterparties



Information from the private sector, financial institutions



- Scan the Internet and Darknet environment for publications, announcements and information
- Request for official registration documents and licenses confirming activity
- Cryptocurrency transaction scanning and analysis and pattern matching



Profile Groups Of Cryptocurrency Actors

Supervised cryptocurrency actors

- Exchanges
- Payment systems
- Exchange offices
- Mining pools

Cryptocurrency users

- Investors
- Miners
- Outlets

Criminogenic and high-risk environment

- DarkMarkets
- Drug trade
- Mixers
- Pyramids
- Malware
- Cybercrime
- Terrorist groups



FATF Recommendations

- VASPs must provide each other the following data:
 - sender's name and details of his digital wallet;
 - the name of the recipient and information about his digital wallet;
 - the physical address of the sender, his passport details or user identifier, which binds him to the company, date or place of birth.
- Anonymous cryptocurrencies delisting
- Termination of unregistered VASP activities



Hybrid Activities Of Most Actors

01

CIRCLE:

- Cross-border payment system
- Currency exchange via cards
- One of the largest OTC sites

02

COINBASE:

- Bitcoin storage – web wallet
- Exchange office

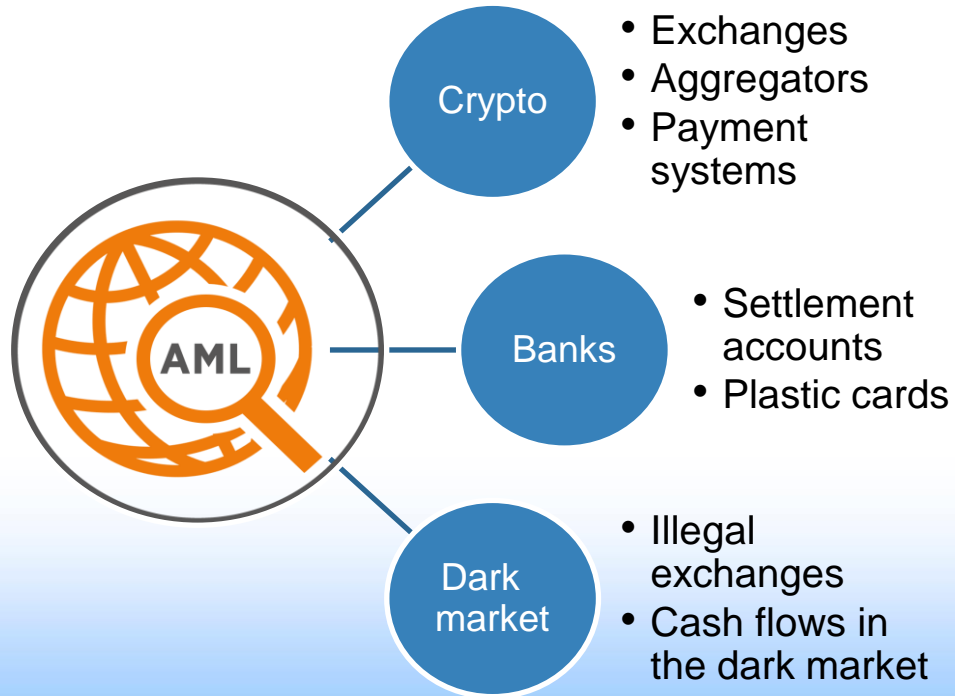
03

XAPO:

- Bitcoin storage – web wallet
- Exchange office
- OTC



Activity types in AML/CFT





AML/CTF work with VASP

- © AML CTF availability control
- © Currency traffic volume analysis for «dirty» crypto
- © VASP reaction to “dirty” crypto



Directions in traditional finance for **AML/CTF**

- © Deanonymization of transactions and matching with bank transactions in the case of private transactions on the purchase and sale of cryptocurrency
- © Matching credit card transactions with transactions in blockchain
- © Control over interacting with “toxic” objects



Identification Of Illegal Objects And Transactions On The Dark Market

- Identification of dark markets
- Mapping
- **Transaction mitigation**



KYT (Know Your Transaction) Solution Know Your Transaction

- © Automation of monitoring of incoming and outgoing cryptocurrency flows, with automatic notification in case of exceeding the risk parameter

Оценка риска

Проверить

Наивысший риск (Входы)

Средневзвешенный риск: 50

Показывать по строк

Поиск:



What Is The Address In Bitcoin?

English | Français | German | Dutch | Português | Русский | Spanish | Italiano | Українська | Türk | Polski | 中文



WalletGenerator.net

Universal Open Source Client-Side Wallet Generator

Выберите валюту : Bitcoin ▼

Единый кошелек

Бумажный кошелек

Несколько кошельков

"Умственный" кошелек

Подробности о кошельке

Поддержка

Generate New Address

Print

Открытый адрес



ОТКРЫТЫЙ

1DtgrfyfNMy1q8JSSjyExSV4o51UNEAMN

Закрытый ключ (в формате импорта в кошелек - WIF)



СЕКРЕТНЫЙ

5Jcj3odVLZAuaCMCft6Gx57TrhbbvFLvUFgoHx4q1NrKivzZ6BE



What Is The Wallet In Bitcoin?

Electrum 2.6.4 - wallet_2

Файл Кошелек Инструменты Помощь

История Отправка Получение Адреса Контакты Консоль

Адрес : Метка : Баланс : Транзакции





▼ Получение

> Потрачено

17AyPVXxC36zFPehEXxB8UBqzwFYAkrGx8	0,	0
13tFdEaX9Sd59citgaXzzJJb4CLEUbTVFo	0,	0
1NuTShwiq3qHhdSbGgToAjHN5MugpFqwly	0,	0
1PZgreuAxKi4CGN34J9z1ZpWAFy41ChLai	0,	0
1AmoyM8hHebDjiJght6Haf6jgkT22KSSBD	0,	0
19KpQ2vXUimANKgVvYJRR8GhxtRSMfUEwS	0,	0
16SEaJfqVFvHZHuUK4QLzgVKWRZNZY55fx	0,	0
1KEWLzCzifThpgycPs3iLZSSumRdtPyxU7	0,	0
1KgcpudBtYJt7UrZSZBGvzY4Q8ubuJ3hvw	0,	0
16ABQnEkjn16Enio6QeAe94FruFvH1XbXA	0,	0
1ECgFHYr8YJDxfz2NV9NfqUGaoAf4Avnan	0,	0
125CGQZaCcn5pxNtmtAh9FosSTgRgkomhY	0,	0
19VBY8W8iaqXutbfkCirFLg1NGgf9RSCnQ	0,	0
1MZ9T2spRhLR1znHuifxaL3JRwPXKCYRHc	0,	0
1MNYLB8eZUsin8gTamxeNA8DXK2HSxQJGY	0,	0
16zyQuKKJ26qy9j63t19SDs5xq6mwTAgGW	0,	0
1dxx4PArxN7Ggrt9qSW7dUavn3QPUnonA	0,	0
13zqAkApv5et45SLZLjXWhxfgoYfA9tbp7	0,	0
19BKGEEwcbqufnmuPX7dYpzR4T1hYsLbZ45	0,	0
1H17FgsyWf67JmeJ3LBWnHc9nCExFVNjAw	0,	0

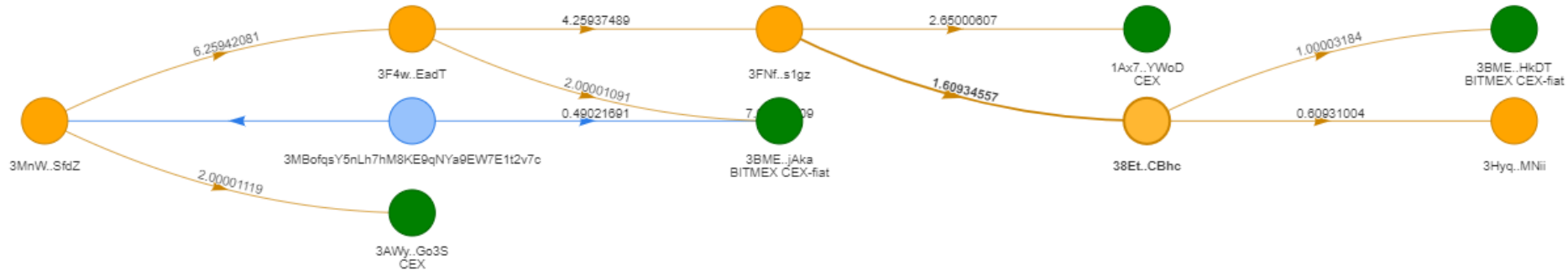
> Сдача

Баланс: 0, BTC (0.00 USD) 1 BTC~611.88 USD

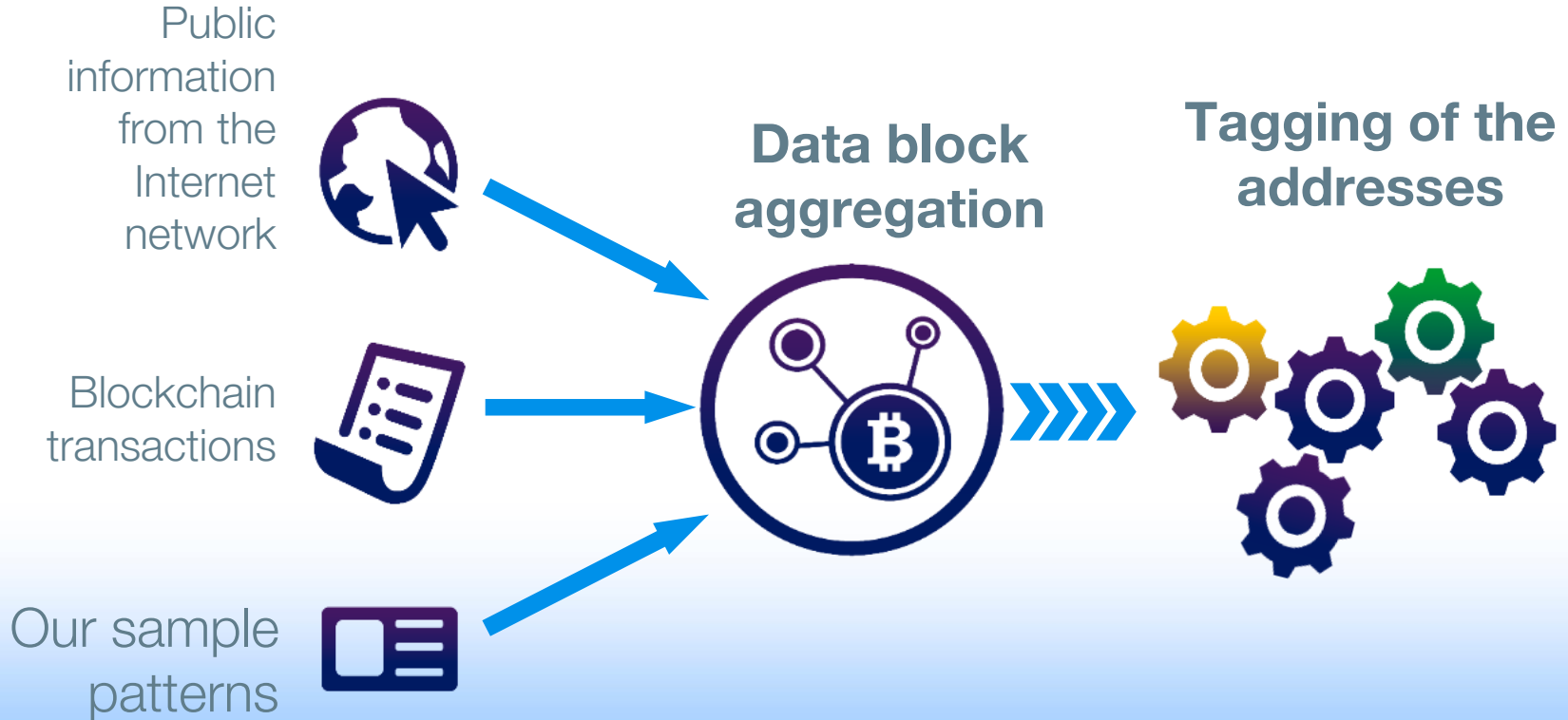


“Follow The Money” With The Tracking Feature





Composition Of Analytical Data





Natural language processing algorithm (NLP)

media

Crimes And Cryptocurrency Are Global





International Cooperation To Solve The Following Problems



Counteraction to attempts to hide funds

Exchange of information on criminal operators and funds



Exchange of information on service providers for cryptocurrency assets



Thank you for your attention!

Alex Yurov

Chief Expert Blockchain research

Lebedev Physical Institute RAS



Currency.com

***Practical Application of AML/CFT Measures
by Cryptocurrency Platform Operator in the
Republic of Belarus – Prospects of
Regulation of these Measures***

General Information on Currency Com Bel LLC and Currency.Com Project

Currency Com Bel LLC is the business entity established in Belarus for implementation of the **Currency.com investment project** (resident of the High Technology Park).

«Currency.com» is the **international project** implemented with the application of the **distributed ledger (blockchain) technologies** and use of **cryptocurrencies and other tokens**.

Currency.com involves **development and commercialization of software** intended for making **investments through carrying out transactions with tokens**.

In the Currency.com project framework, Currency Com Bel **issues and offers its own tokens** (on Ethereum blockchain) and also **plans to provide ICO** (token issuing and offering) **services** to other persons.



HTP – Organized Token Market Environment

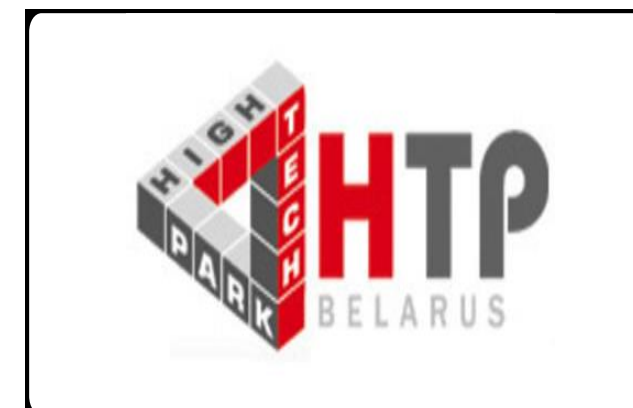
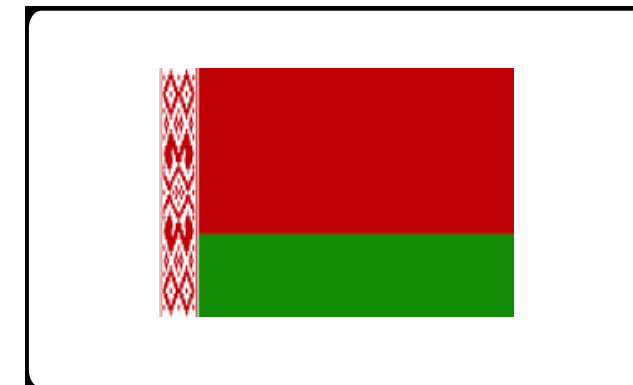


Currency.com project is **implemented mainly under the jurisdiction of Belarus** where the **comprehensive regime of high-quality and liberal regulation of circulation of tokens** has been established. This regulatory regime is underpinned by:

- RB Presidential Decree No.8 on Development of Digital Economy issued on 21.12.2017;
- Regulations issued by the HTP Supervisory Board.

High Technology Park (HTP) is the **organized token market** operational environment.

Professional token market participants shall necessarily be registered as the HTP residents.



14:40

85 %



currency.com



1. Общество с ограниченной ответственностью «Карренси Ком Бел» (УНП 193130368) расположено по адресу: 220030, г.Минск, ул. Интернациональная, 36-1, офис 724, помещение 2.
2. ООО «Карренси Ком Бел» является резидентом Парка высоких технологий (решение о регистрации в качестве резидента Парка высоких технологий, протокол №08/НС-6пр от 19 декабря 2018 г.) и осуществляет свою деятельность в соответствии с Декретом Президента Республики Беларусь от 21 декабря 2017 г. № 8



HTP – Organized Token Market Environment

Types of activities of carried out by professional token market participants in the HTP:

1. Provide token issuing and offering services (operate in capacity of ICO organizers);
2. Operate in capacity of cryptocurrency platform operators;
3. Operate in capacity of cryptocurrency exchange operators;
4. Carry out other activities involving tokens as well as issue and offer their own tokens (own ICO).

Currency Com Bel is involved in activities 1, 2 and 4

Definition of virtual asset service provider in the FATF Recommendations:

Any natural or legal person who, as a business, conducts one or more of the following activities or operations for or on behalf of another natural or legal person:

- * exchange between virtual assets and fiat currencies (sale and purchase);
1, 2, 3, 4
- * exchange between one or more forms of virtual assets;
1, 2, 3, 4
- * transfer of virtual assets (on behalf of other persons); 1, 2, 4
- * safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets;
1, 2, 4
- * participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.
1



AML/CFT regulation is provided for in the Regulation on Requirements for Internal Control Rules of the High Technology Park Residents approved by the Resolution of the HTP Supervisory Board on October 23, 2018 (Minutes No.08/NS-5pr).

The Requirements for internal control rules of **forex companies** approved by the RB National Bank Board we used as the template. **Foreign experience was also analyzed.**

- AML/CFT Guidance for Virtual Currencies prepared by **Isle of Man** Gambling Supervision Commission in 2017;
- Consultation paper «Regulating digital currencies under Australia's AML/CTF regime» prepared by the Attorney-General's Department of the **Australian** Government 2016;
- **FATF** Guidance for a Risk-based approach to virtual currencies of June 2015;
- Tracfin (**France**) recommendations to prevent virtual currencies from being used for fraudulent purposes and money laundering «Regulating virtual currencies» 2014;
- **FinCEN** Guidance «Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies» 2013;
- Regulations of the Superintendent of Financial Services: Virtual Currencies. Adopted by the **New York** State Department of Financial Services.

Some **AML/CFT measures** were borrowed from other **practices applicable to transactions with tokens**, including:

- Methods of verification of identification data, such as obtaining information on customers from **commercial databases** (World-Check, Accuity, Dow Jones and others); tracing **customer's IP-address**; using **web-ID procedure** when carrying out transactions above certain threshold;
- Suspicious financial transaction indicators, such as use by customers of anonymizer software, IP mixers, coin mixers and other **anonymizer software** for transferring tokens (including virtual wallets, which make it impossible to trace transactions, such as Dark Wallet); use of virtual wallet addresses on such websites as **Silk Road, AlphaBay, Hansa, Dream Market, CGMC**, etc. for carrying out financial transactions;
- Software used for **analyzing transactions on blockchain** (Elliptic, Chainalysis, Coinfirm, etc.);
- Refusal to deal in tokens that provide for **complete anonymity** of transactions (Dash, etc.);
- **Independent testing (assessment)** of internal control rules.



AML/CFT Requirements for HTP Residents' Activities

(Requirements for Internal Control Rules)



ML/TF risk management procedures
(three-pronged model: (1) customer profile risk; (2) geographic risk; (3) transaction risk)

Identification and verification of all customers carrying out financial transactions

AML compliance officer
(appropriate education, experience of working in economic or legal area, AML training)

Refusal to carry out transaction
(transactions with anonymous tokens and with tokens in amount exceeding 2000 base units where payments are made by way of wire transfer or E-money transfer, etc.)

AML / KYC

Software for monitoring transactions and identifying those related to criminal transactional activities
(Elliptic, Chainalysis, Coinfirm, etc.)

Possibility of freezing funds and (or) blocking financial transactions of persons linked to terrorist activity

Filing special data forms with the financial monitoring agency
(when financial transactions are identified as those subject to special control, when freezing funds or blocking financial transactions)

Identification of financial transactions that are subject to special control
(cross-checking each transaction against suspicious financial transaction criteria and indicators)

Development of AML/CFT Regulation of HTP Residents

1. Implementation framework: **Interpretive Note to Recommendation 15 on New Technologies and Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers of 21 June 2019** in full scope.
2. It is proposed to permit the HTP residents to use **foreign identification systems** (digital ID, for example: GBG, England) that are not inconsistent with the FATF Recommendations.

Identification system is a combination of data banks, information technologies, software and hardware intended for collecting, processing, storing and providing information on customers and customers' representatives for their identification that enables to obtain customer identification data without receipt of documents containing such data (copies, images therefor) from customers.

3. It is proposed to permit the HTP residents to use the extended list of documents that may serve as the source of identification data – apart from the standard ID document, such documents should also include **driving licenses** (other similar documents), **voter registration certificates**, **taxpayer cards**, **employment cards** issued in the country of origin or permanent residence of a natural persons who is subject to identification.

According to FATF Recommendation 11 documents used for identification of customers include, apart from passports, such official ID documents as *identity cards, driving licenses and other similar documents*.

4. It is proposed to permit the HTP residents to **complete identification of customers after establishing contractual (business) relationships with them**.

Development of AML/CFT Regulation: Delayed Completion of Verification

It is proposed to permit the HTP residents engaged in transactions with tokens to **complete verification (of identity) of customers within 15 days after establishment of business relationships with them, or before tokens are transferred to (withdrawn by) customers, if they requests to do so prior to expiration of the 15-days period.**

Practical experience: Cyprus (CySEC No.C157 dated 24.06.2016, page 3), and also Malta and Lithuania.

FATF Recommendation 10:

“Countries may permit financial institutions to complete the verification of customers as soon as reasonably practicable following the establishment of the relationship, where the **money laundering and terrorist financing risks are effectively managed** and where **this is essential not to interrupt the normal conduct of business**”.

A) *Why ML and TF risks are effectively managed*

A customer hands over funds (e.g. moneys, tokens) to a HTP resident, but, **until his/her verification is completed, such customer cannot receive them bank (withdraw) and dispose of them at his/her own discretion and, therefore is unable to launder proceeds or to finance terrorists.**

B) *Why this is essential not to interrupt normal conduct of business:*

Item 11 of Interpretive Note to Recommendation 10:

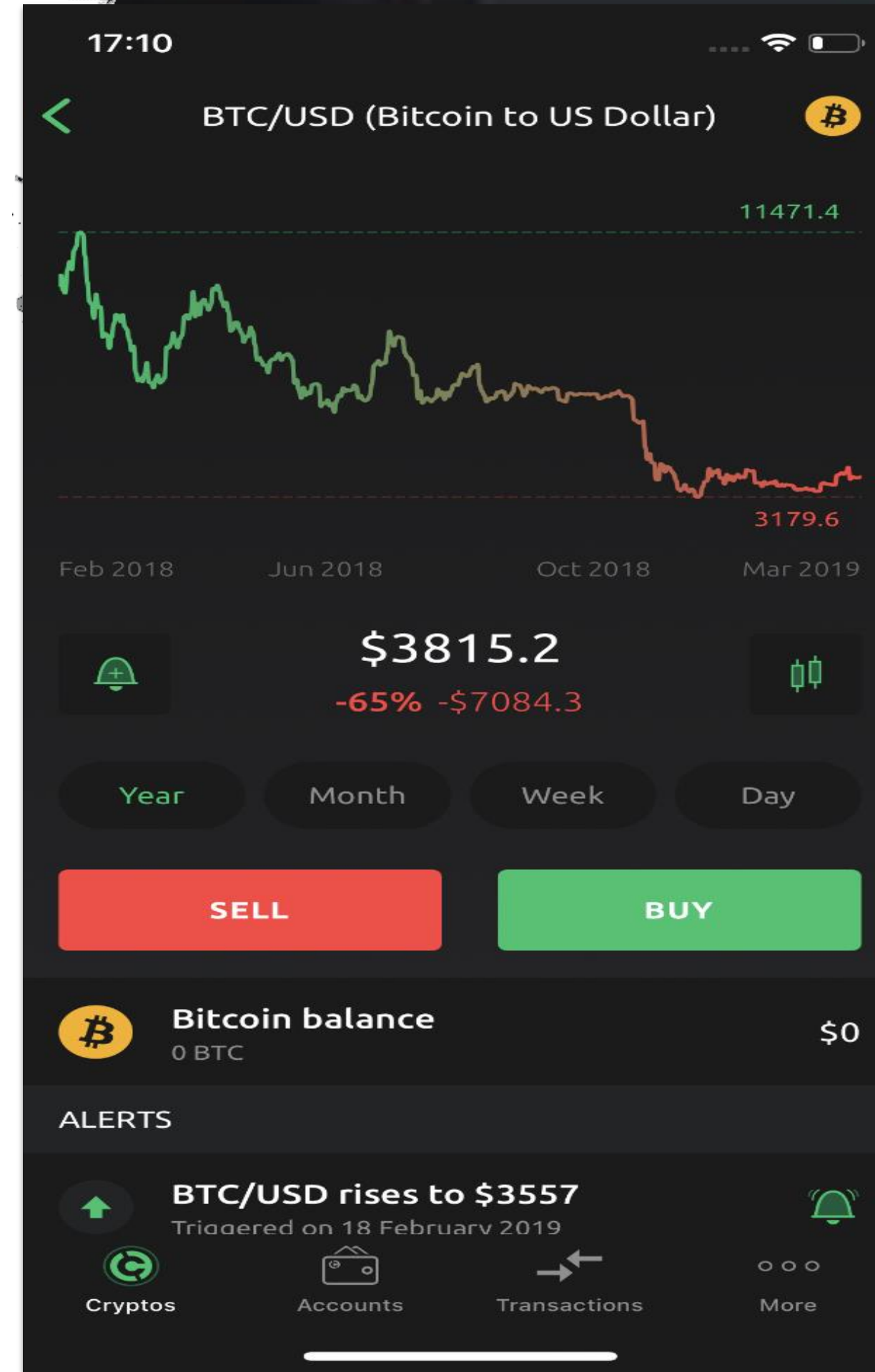
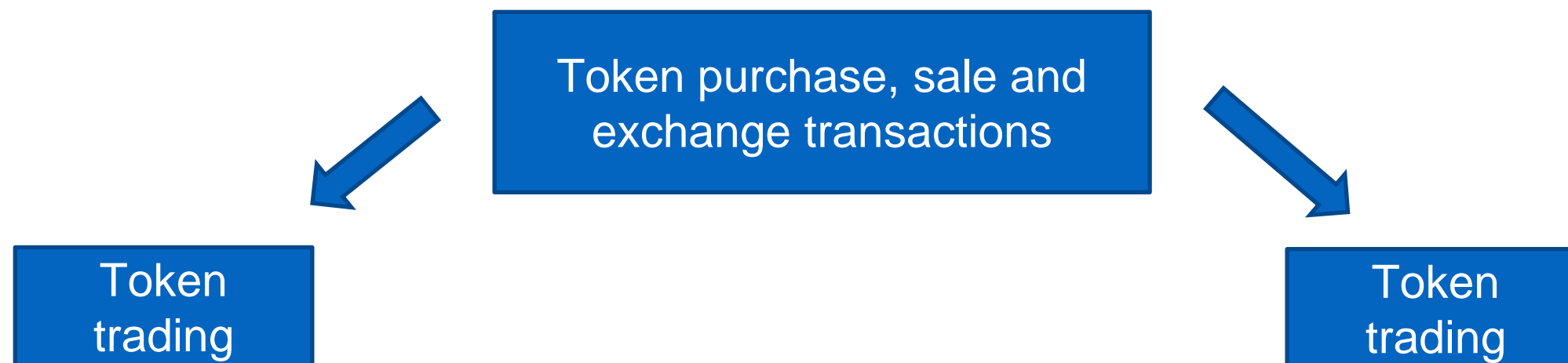
“Examples of the types of circumstances where it would be permissible for verification to be completed after the establishment of the business relationship, because it would be essential not to interrupt the normal conduct of business, include **non face-to-face business**. The HTP residents engaged in activities with tokens always deal with customers remotely (i.e. without face-to-face contact).

Core Currency.com Project Software



1. Currenyc.com cryptocurrency trading platform (cryptocurrency exchange);
2. Currency.com Exchange Mobile Application (cryptocurrency exchange for mobile devices);
3. Currency.com – Buy Bitcoin (cryptocurrency exchange for mobile devices).

Most transactions carried out with the use of this software involve sale, purchase, and exchange of tokens.



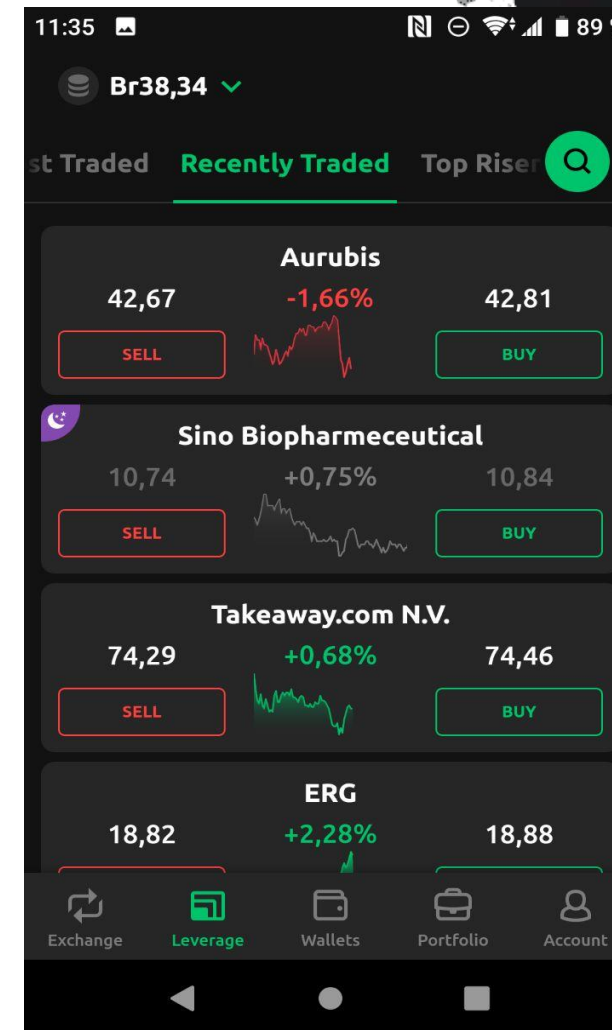
Core Currency.com Project Software



Currency Com Bel **software** enables to carry out transactions with:

1) Cryptocurrencies

- *Bitcoin;*
- *Etherium;*
- *Litecoin.*



2) Tokens issued by Currency Com Bel:

- *Currency representing tokens;*
- *Tokenized exchange assets;*
- *Tokenized bonds.*

In the process of arranging and carrying out transactions with tokens, Currency Com Bel operates as the **centralized cryptocurrency platform**.

Currency Com Bel **accepts customers' funds** (fiat money, E-money, tokens) **to its bank accounts, e-wallets and e-wallet addresses** to enable payments under carried out transactions.



Currency Com Bel Internal Control System

- ***Identification*** (before establishing business relationships) ***and verification*** of all customers;
- ***Keeping customer identification data*** (including those obtained as a results of their verification and updating);
- ***Monitoring*** all financial transactions of customers for identifying and documenting financial transactions that are subject to special control and reporting relevant information to the financial monitoring agency;
- Taking measures, that are reasonable and available in given circumstances, to ***establish sources (of origin)*** of funds and tokens of customers.



Management of ML-Related Risks

- Management is performed with application of ***risk-based approach***;
- Measures are taken to categorize, describe and assess risk with due consideration for risk ***increasing (reducing)*** factors;
- Risk of dealing with a customer is assessed based on the ***three-level risk scale*** (low, medium and high);
- ***Three-pronged*** risk distribution ***model*** is used that includes three vectors: customer profile risk, geographic risk and transaction risk;
- ***Matrix*** based on the three-pronged risk distribution model (with application of the point scale) is used for assigning the final level (degree) of risk to customers.



Customer Identification

Before onboarding, Currency Com Bel obtains the following information from customers:

- Last name, first name and patronymic (if any);
- Nationality (citizenship);
- Date and place of birth;
- Residential address and (or) address where a customer temporarily stays;
- Details of ID document;
- Information on beneficiary (if any);
- Contact details of customer (E-mail address).

Where Currency Com Bel obtains the aforementioned data from a natural person, it requests such individual to ***clarify*** whether he/she acts on his/her own behalf and for his/her own benefit.



Identification Procedure

State 1 of Identification:

A customer is requested to complete the **electronic registration card** accessible through the web-interface.

This card shall be completed based on the ID document (passport, identity card, residence permit certificate).

Stage 2 of Identification:

A customer is requested to send the **graphic images** of the ID document pages containing personal details and information on place of residence, and where place of staying differs from the official place of residence (or is not indicated), the **graphic images** of documents confirming actual residence (utility bills, etc.).



Web-ID

Web-ID procedure (***type of remote identification by way of video conferencing on the Internet***) may be used instead of completion of the electronic registration card for verification purposes.

In course of this procedure, a customer ***shall keep his/her ID document and other necessary documents in front of web-camera***, so that his/her face can be compared with photo-picture contained in the ID document, and other information contained in the ID and other documents can be obtained (read) for verifying veracity of the previously provided data.

Currency Com Bel necessarily conducts the web-ID procedure before carrying out transactions involving sale and purchase of tokens in amount equal to or exceeding 5,000 base units (**approximately USD 61,500**)



Mandatory Measures

Currency Com Bel ***verifies information on customers (before onboarding)*** in order to:

- Identify, among customers, persons ***who are foreign politically exposed persons, officials of international organizations, persons holding offices*** included in the list of the RB public positions adopted by the RB President, their family members and close associates;
- Identify, among customers, persons ***who are involved in terrorist activities, linked to proliferation of weapons of mass destruction or controlled by such persons*** (the relevant list is posted on the website of the RB State Security Committee).



Questionnaires

- The ***customer questionnaires*** have been developed (based on the identification questionnaire) ***for each group (category) of customers*** (natural persons, individual entrepreneurs, legal entities).
- The questionnaire may be **standard or extended** (depending on level (degree) of risk of dealing with a customer).
- The questionnaires are completed ***electronically*** with the use of the **User admin area** software.



User Admin Area

#10827419 -



10 ☐ USD

	Type	Name	Curr.	Equity	UPL	Margin	Equity / Margin	Balance	Available for WD
		Total	USD						0.00
No records found									
No records found									

Details

Balances

Positions

Positions History

Orders

Orders History

Exchange Orders

Exchange Orders History

Transactions

Sessions Log

Communication

Locale	en	Print
Email		
User Type	RETAIL	
Qualified investor	No	
LTV Category		
Invite Code		
Gender		
First Name		
Mid Name		
Last Name		
Second Surname		
Previous Last Name		
Date of Birth	-	
Country of Birth		
Country of residence	United States Minor Outlying Islands	

Categories: [Edit](#)

CAD: - not assigned - [Set](#)

Status HTP - NEW

Account status: NEW

License	HTP - NEW
Appropriateness Score	0
Target Market Score	
Registered	2019-09-22 21:53:37
Email Confirmed	2019-09-22 21:55:08
First Deposit	
Reg Form Submitted	2019-09-22 21:53:37 REGULAR
Terms Confirmed	2019-09-22 21:53:37 #4
AML Risk	Check History

[Passport](#) [Upload](#)



User Admin Area

- ***Keeping history*** of customer questionnaires with possibility of viewing changes and (or) updates (*inter alia*, based on results of verification) and dates of such changes/ updates in respect of each customer;
- ***Keeping history of updates*** of a customer questionnaire (who and when updated a customer questionnaire);
- ***Keeping register of changes*** (when, by whom and what changes were made in customer questionnaires);
- ***Available search engines*** allow for selecting (retrieving) customer questionnaires that meet the preset parameters;
- ***Displaying information links*** between and among customers;
- ***Printing*** customer questionnaires.



Verification

Currency Com Bel applies the following **measures** for verification purposes:

- **Cross-checks** the identification data provided by a customer against information obtained on such customer from publicly accessible and other information sources, *inter alia*, from social media;
- **Contacts** a customer by phone, mail, E-mail or through videoconferencing on the Internet;
- **Traces** customer's **IP-address**;
- **Examines publicly accessible information sources** (*inter alia*, the Internet) for any negative information on a customer;
- Applies the **web-ID procedure** for verifying veracity of the identification data previously provided by a customer;
- Receives a **photo-picture of a customer along with his/her ID document** opened at pages containing personal details and photo-picture sent by the customer from the e-mail address indicated during registration.



Monitoring Procedure

For monitoring purposes, Currency Com Bel has developed and implemented the ***system of alerts*** that enable to **automatically identify transactions that are subject to special control**, when, for example:

- Value of customer transactions reaches certain threshold amount (USD 10,000 equivalent and more);
- Customer uses more than 1 bank payment card for making payments to (settlements with) Currency Com Bel;
- Customer uses more than 1 virtual wallet address for making payments to (settlements with) Currency Com Bel;
- Several customers use the same virtual wallet address for making payments to (settlements with) Currency Com Bel, etc.



Monitoring Transactions with Tokens

Currency Com Bel uses the **software** (Coinfirm and Crystal) ***that summarizes and analyzes the use by customers*** (potential customers) ***of their virtual wallet addresses*** (identifiers), and also ***assesses the risk*** of use of customers' (potential customers') virtual wallet addresses (identifiers) ***for conducting (participating in) illegal activities***.



Statistics

Since 15.01.2019 through 24.09.2019, Currency Com Bel identified **86 suspicious financial transactions** that were reported to the financial monitoring agency.

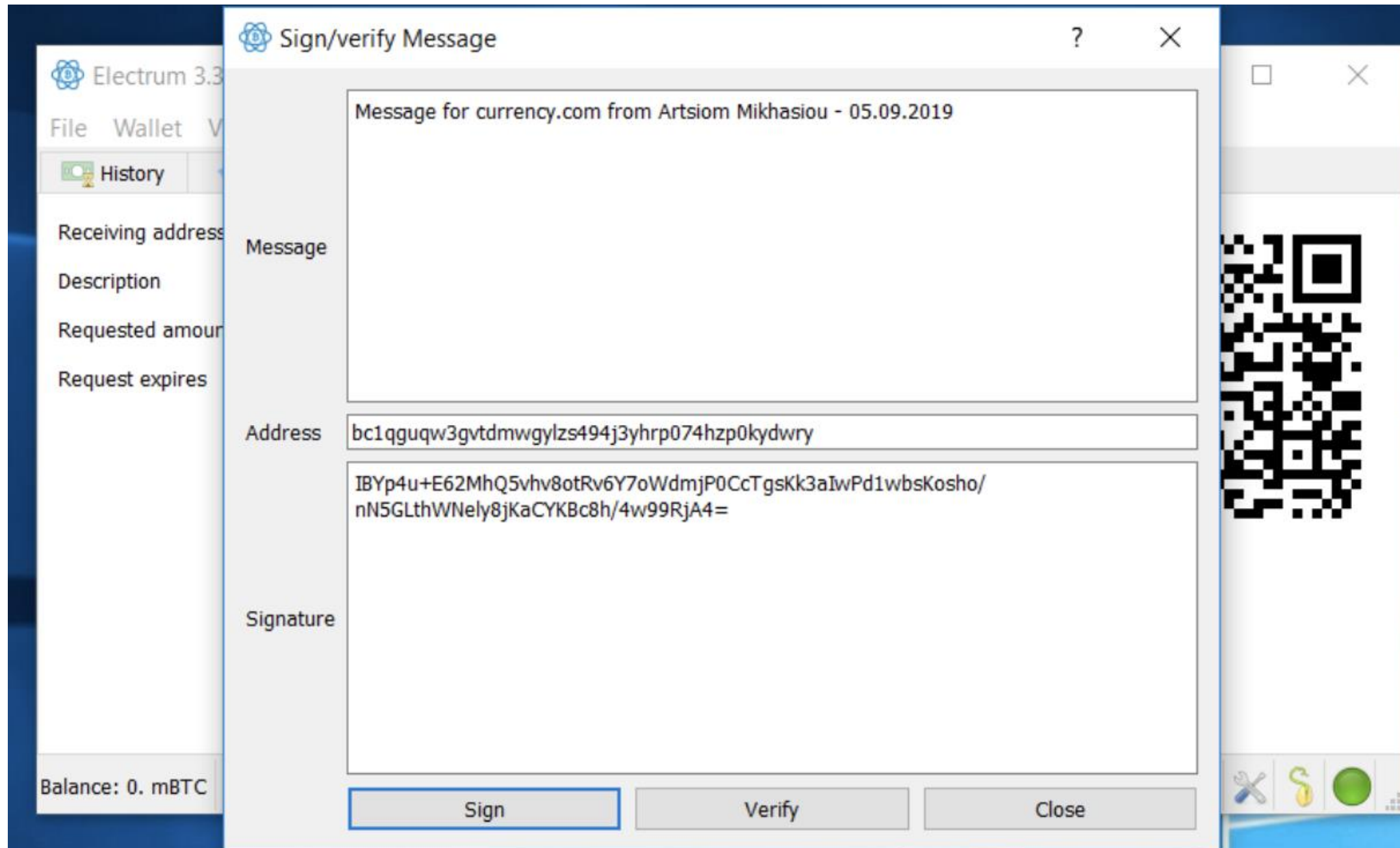
The most common suspicious indicators included the following:

- 1) For the purposes of making payments to the HTP resident or to other persons through the HTP resident, a customer uses a bank account or e-wallet opened in an offshore zone, or uses e-wallet owned by a third party or a bank account opened in a country other than the country of its registration (his/her residence);
- 2) A customer provides information that raises suspicions, including information which verification is impossible (extremely difficult) or very expensive;
- 3) A customer provides documents (copies thereof) that raise doubts about their authenticity (veracity) or provides false documents;
- 4) A customer refuses to provide the requested documents (information) without good reason, or unreasonably delays submission of such documents (information), or is over concerned about confidentiality issues;
- 5) A customer provides a written confirmation indicating absence of a third party for the benefit of whom a financial transaction is carried out, where, based on the inquiries with the customer on this issue, the HTP resident is still convinced (suspects) that such third party exists.



Operational problems

2) Verification of ownership of customers' virtual wallet addresses:



Thank You for Attention!

**Aleksandr Petrovich Shevchenko,
Ph.D. in Law
Manager of Currency Com Bel LLC**

**Darya Dmitrievna Simonenko
Lead Financial Monitoring Specialist of
Currency Com Bel LLC**



Currency.com



AML/CFT: From Data to Solutions

Shifting Focus to Online Control

“We are living at the height of a data deluge”

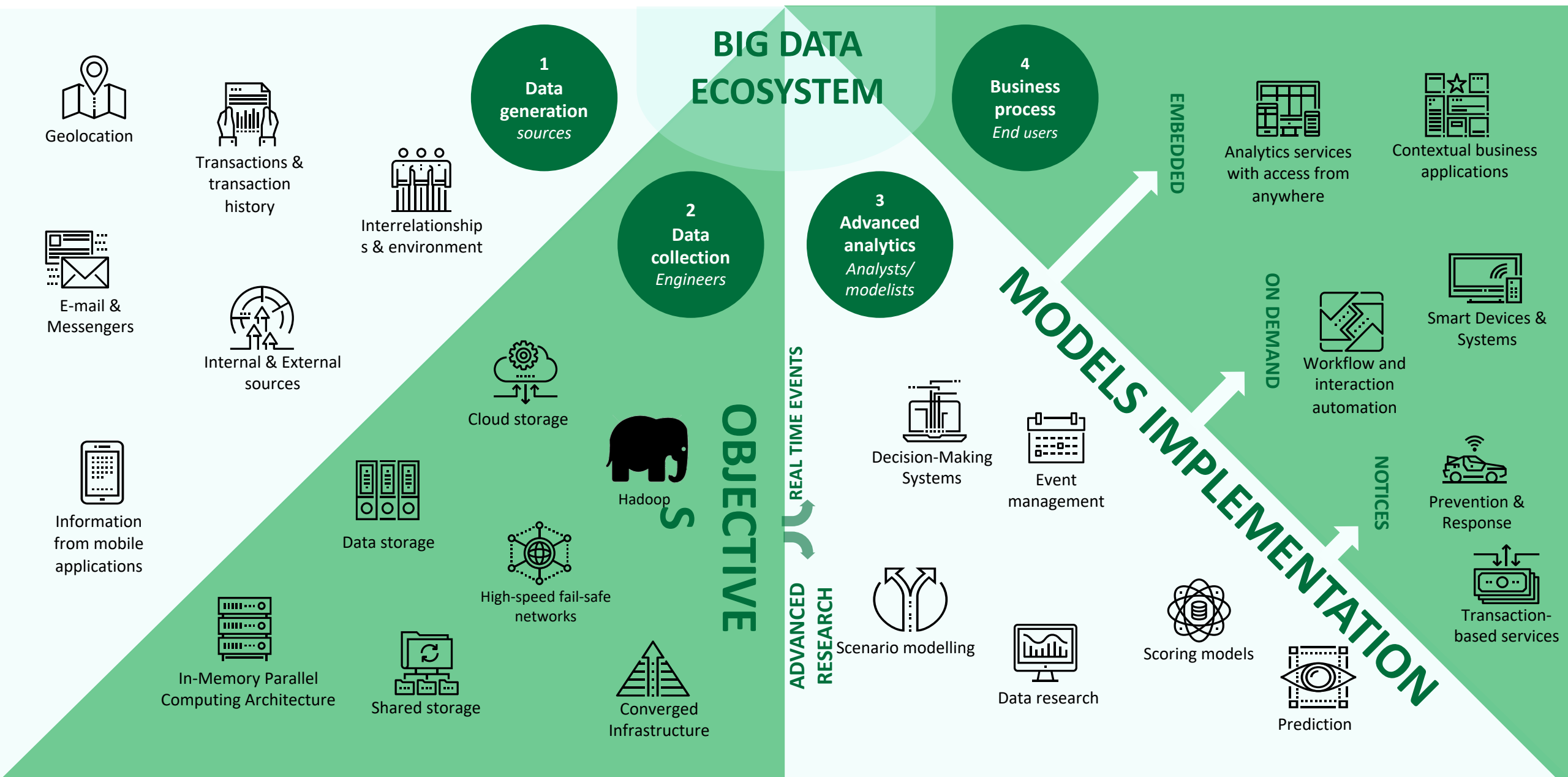
2.5

quintillion (10^{18}) bytes of data
are generated daily

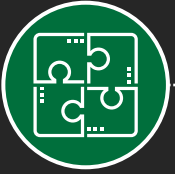
More than
90 %
of information

that we're currently storing
was created in the last
decade alone

From Data to Solutions



Post-Control



GENERAL RULES

- Legislation
- CBR Guidelines



CUSTOMER PROFILE AND ENVIRONMENT

- Negative profile
- Negative environment, counterparties



TRANSACTIONAL CHARACTERISTICS

- Transactional features
- Negative patterns/schemes



SCORING

- Continuous addition of new data sources
- Selection of high-risk segments for future analysis



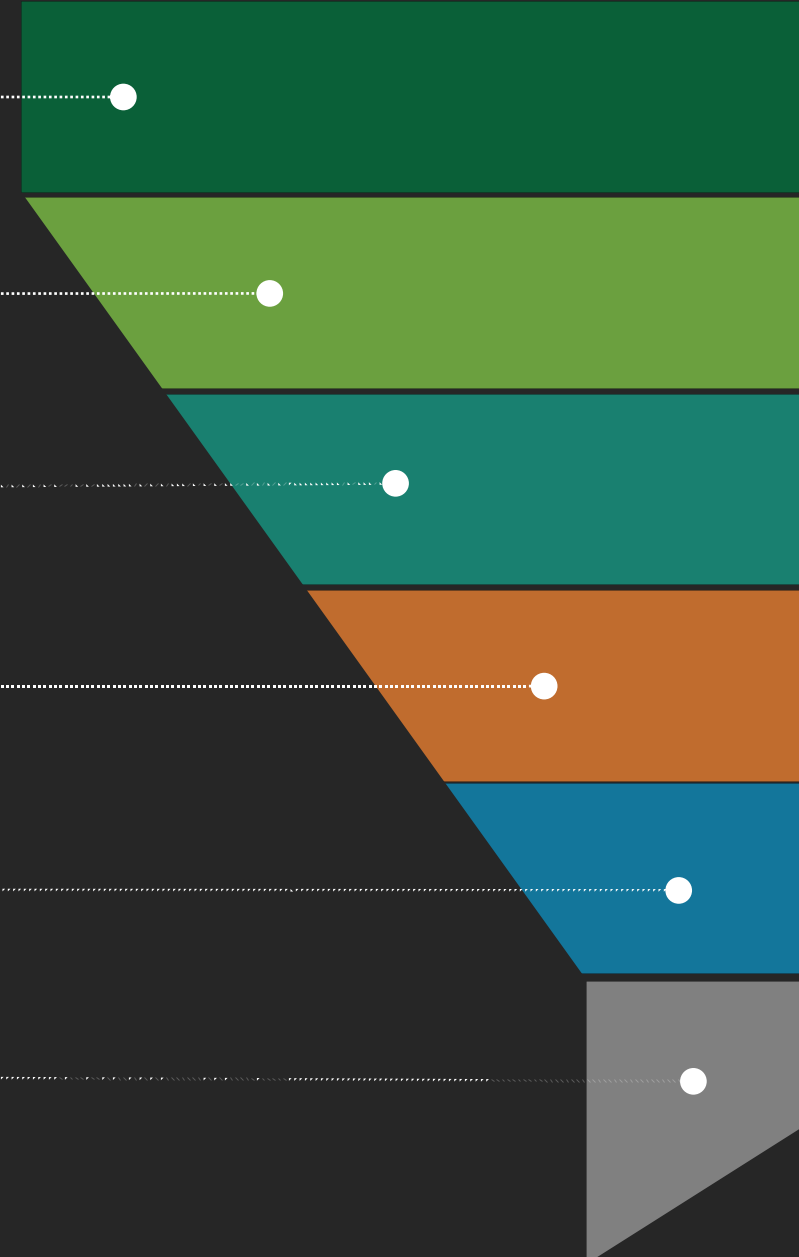
CUSTOMER SEGMENTATION

- Each model works for its own segment
- Different models cover different patterns/schemes



SORTING

- Volume of potentially dubious transactions
- 85% hit rate





Ensemble of models for a new client joining the Bank

Identification of AML risk clients before they are onboarded for banking



Early identification models for AML risk clients/ patterns

Decreased level of the Bank's involvement



Documents Recognition

Reduction in man-hours when analyzing documents



Models to detect anomalies

Decreased level of the Bank's involvement



Prediction of AML activity turnover

Assistance in decision-making from a compliance employee

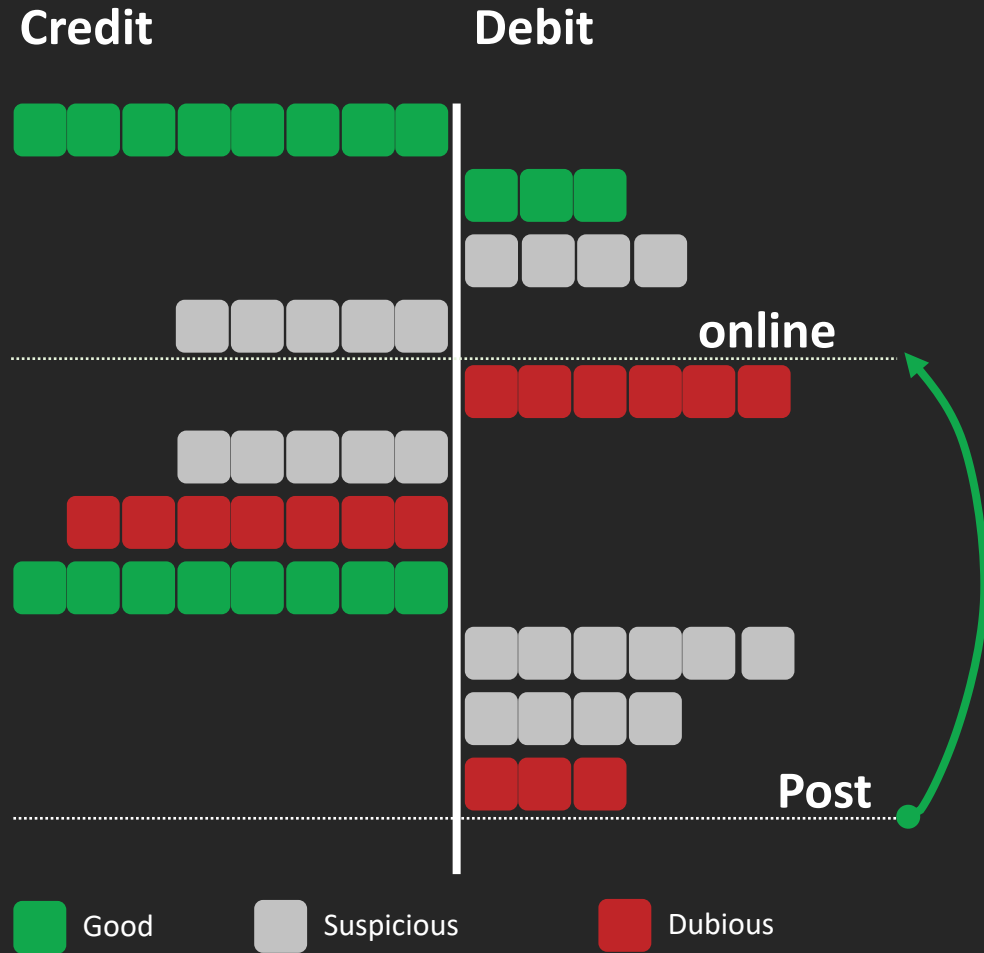


Start models

Decreased average bill for the new AML client

AI Elements in AML

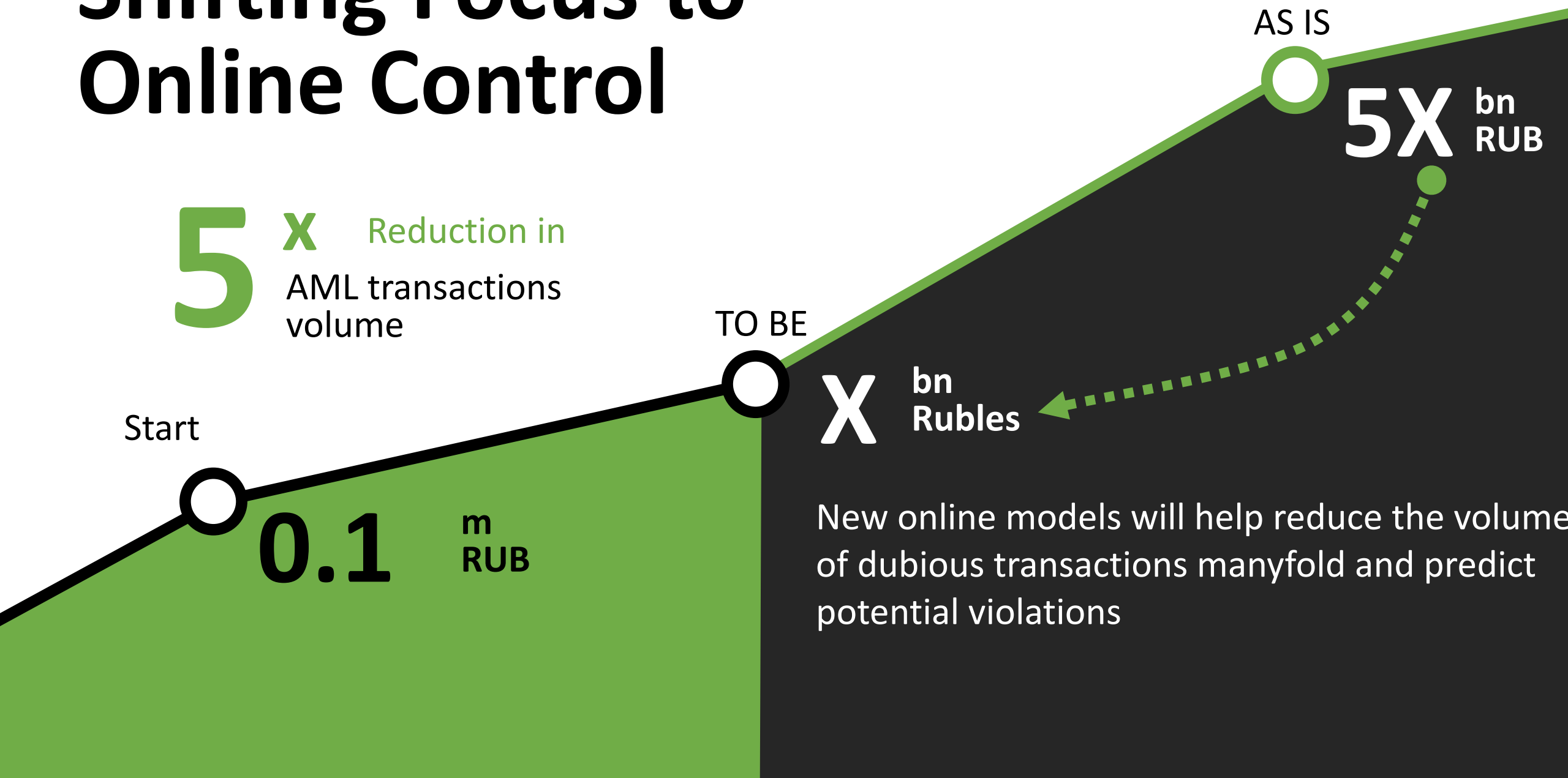
Shifting Focus to Online Control



Main objective:
Shifting focus from post-control to online

New online models will help reduce the volume of dubious transactions manyfold

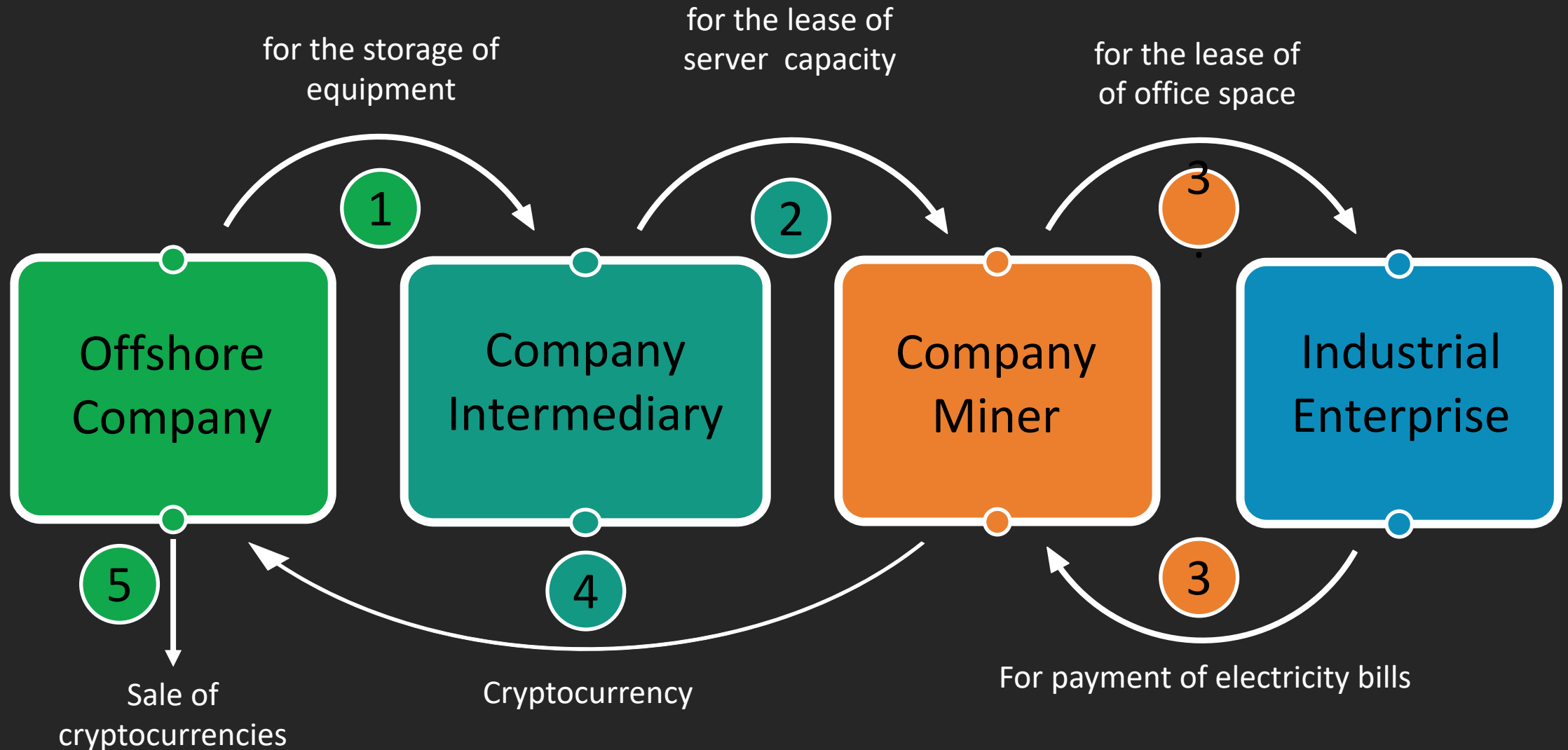
Shifting Focus to Online Control



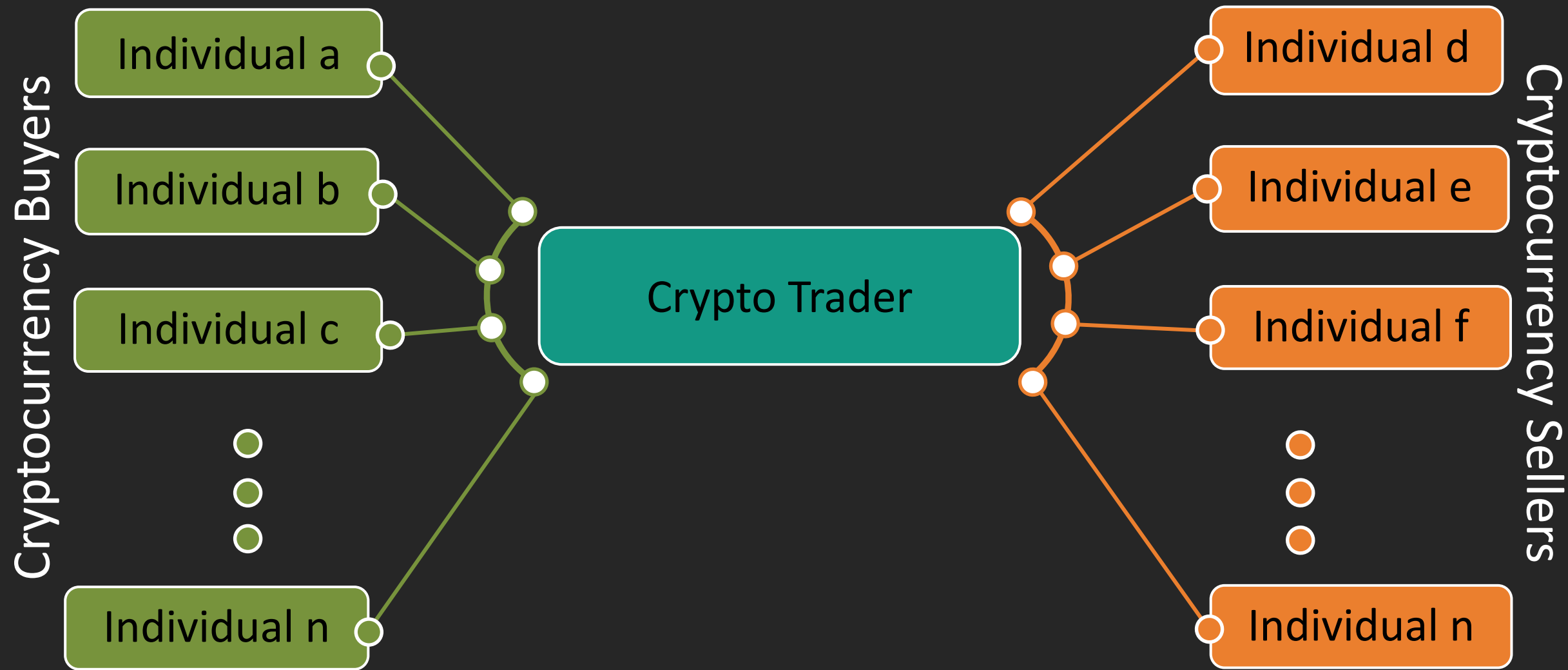


AML/CFT: Cryptocurrency Use Risks

Risk of Capital Outflow Abroad Using Cryptocurrencies



Risk of Criminal Proceeds Laundering Using Cryptocurrencies



September 2019

Suspicious transactions with financial assets

Executive summary



Money laundering has been expanding footprint on the **financial markets** in the post-2008 period against the backdrop of banking regulations toughening. Being **less regulated** and **more sophisticated**, traded financial instruments are **at risk of being used for ML**. Risk-oriented approach coupled with research allows **educing** legally-looking **ML operations** from **regular** ones.

The background is a photograph of a person's hands in a dark suit holding a brown paper envelope over a wooden table. Another person's hands are visible in the lower right, gesturing. The scene is dimly lit, with a strong shadow cast by the envelope.

How are NFIs involved in money laundering process

From banks to financial market

How it works?

Funds originated by illegal activities are gradually converted into legitimate assets via a series of transactions

Key benefits:

- Execution velocity
- Options variety

How NFIs are involved?



1. Crime

origination of funds through
illegal activities

2. Allocation

funds allocation
in the financial market

3. Split

mixing up source
of funds traces

4. Integration

funds and assets
become legitimate

Illiquid financial assets as a money laundering tool

Liquidity - ability of an asset to be sold in a short
time without drastic change in price

Russian market



Liquidity of the marker is weak

After the 2008-2009 crisis international investors left the market

The majority of deals are executed on OTC

Exchange quotations do not reflect the real market situation

In absence of credible market data

Counterparties control the price

Liquid assets:

20 – 25 stocks

accounts for 60%
of the market

70 bonds

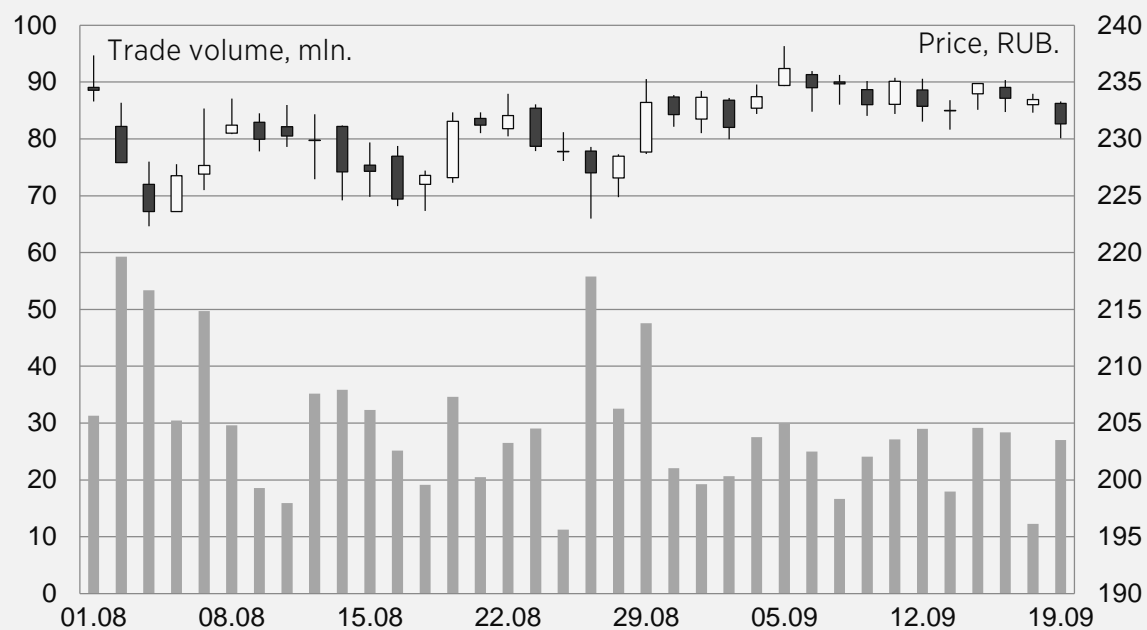
accounts for 30-
35% of the market

As the result, criminals may enter into transactions in order to distort stock market data and evade AML/CFT control

Difference in securities trading history

High-liquid security

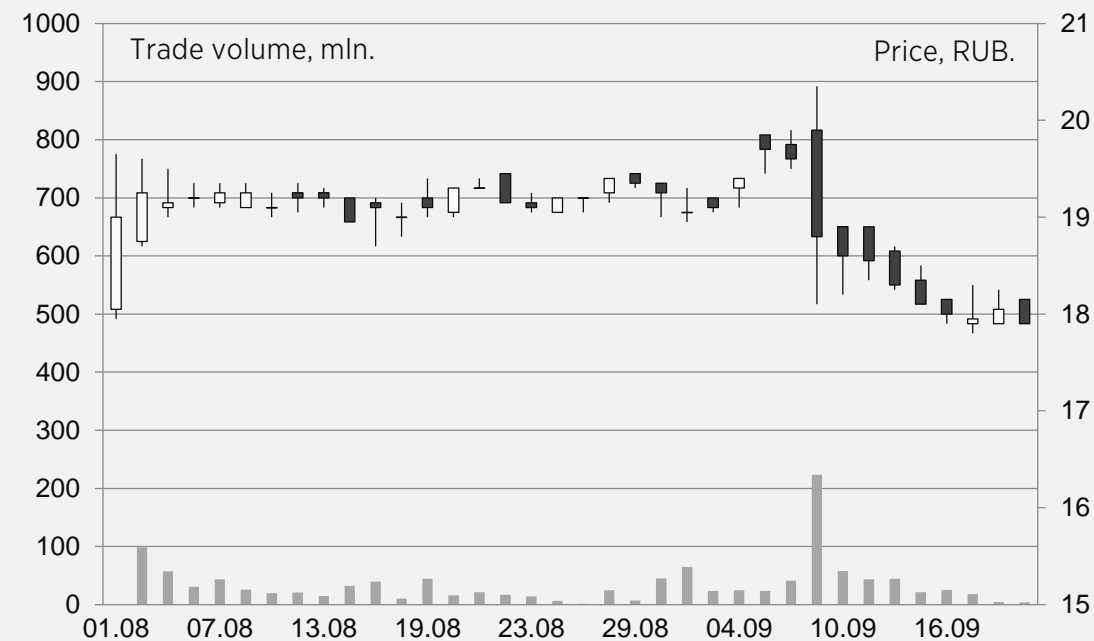
TNS «Gazprom»



Source: Bloomberg

Low-liquid security

TNS «Permenergosbyt»



Source: Bloomberg

Main purposes of using non-liquid securities

1. Capital withdrawal out from Russian Federation
2. Change of ownership
3. Tax evasion (tax optimization)
4. Settlement operations

Capital withdrawal out of Russia

How does it happen?

Two professional participants conclude a counterparty transaction with a non-liquid asset and a large amount

What is typical about capital withdrawal?

- ✓ the transaction is concluded on stock exchange or OTC;
- ✓ the counterparty is a Russian professional participant or a financial organization from a country highly rated by FATF;
- ✓ large amount;
- ✓ as a result, the asset is transferred abroad

Which instruments are used?

Stocks / Bonds / Investment Shares / Derivatives

Change of ownership



How does it happen?

Securities are transferred from one depository to another by concluding an OTC transaction.

What is typical about change of ownership?

- ✓ OTC transaction;
- ✓ the change of the depository means the change of jurisdiction;
- ✓ the asset price varies and depends on the offenders' aims;
- ✓ no real payment.

Which instruments are used?

Stocks / Bonds

Tax evasion



How does it happen?

Using a professional market participant, a natural or legal entity concludes a series of transactions resulting profit to the one party and loss to the other (decrease in taxable profit).

What is typical about tax evasion?

- ✓ the transactions are concluded on stock exchange;
- ✓ transactions among controlled entities;
- ✓ several, similar transactions with the same party;
- ✓ as a result, one party always “wins” and the other always “loses”.

Which instruments are used?

Stocks / Bonds / Investment Shares / Derivatives

Settlement operations



How does it happen?

Using a professional market participant the client pays a significant amount for non-liquid securities to hide a goods services payment.

What is typical for settlement operations?

- ✓ the transaction is concluded on stock exchange or OTC;
- ✓ a large amount;
- ✓ the payment is made with the help of a professional market participant.

Which instruments are used?

Stocks / Bonds / Investment Shares / Derivatives

NFIs should pay attention to:



Financial instrument

Trading history, Volume of issue, Spread

Issuer (financials, business), Exchange (how quickly and cheaply securities can be listed)

Participant

Large number of intermediaries involved (administrators, depositories, banks, etc.)

Readiness of counterparties to disclose the Ultimate Beneficial Owner

Jurisdiction

Change of jurisdiction

Assets are transferred to a low-tax jurisdiction

Currency

Transaction currency differs from the currency instrument is traded in

Example of low-liquid securities automated monitoring
(A client buys a low-liquid security for a large amount)

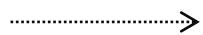
The number of other transactions is small.

One-time OTC transaction



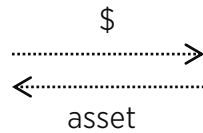
1

Money is debited to the brokerage account



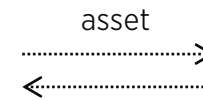
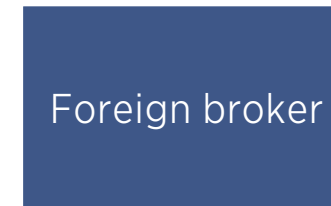
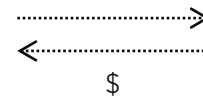
2

Asset purchase order



2

Asset sale order



Result: \$50K is received on the bank account of Non-resident Company outside Russia

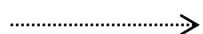
Asset – illiquid Eurobond. No supply/demand. Impossible to determine the market price (=0)

Conclusive trades



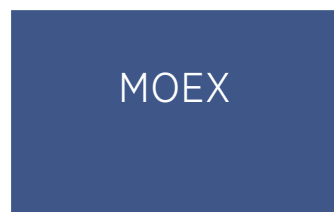
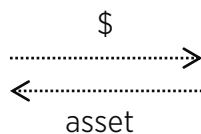
1

Money is debited to the brokerage account



2

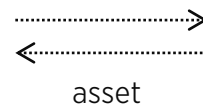
Asset purchase order
150 orders, V – 450 000 securities



1) 72 RUB./per asset
⋮
54) 250 RUB./per asset
⋮
100) 400 RUB./per asset
⋮
150) 480 RUB./per asset

2

Asset sale order
150 orders, V – 450 000 securities



Result: 1) price 2 – 480 RUB./piece 2) ₸200 mln. is received on the bank account of Company B

Asset – listed illiquid corporate bond, market price – 72 RUB./per asset

Multicomponent scheme



1

Money is debited to the brokerage account

3

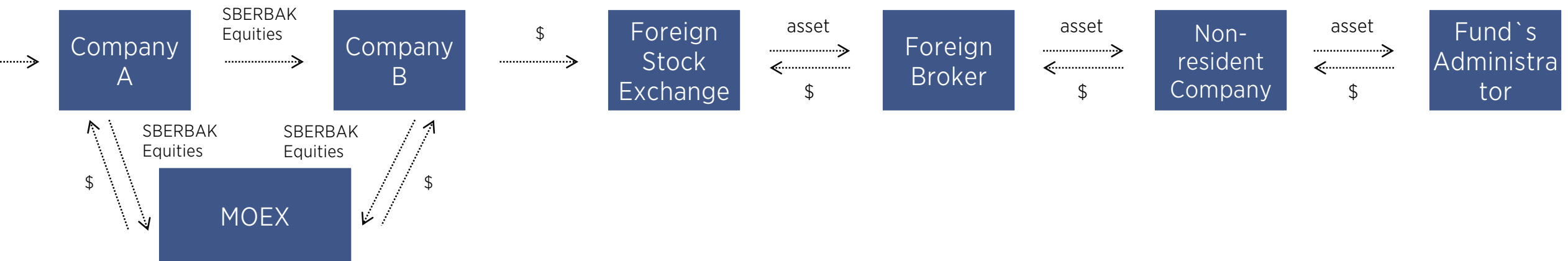
Custody transfer.
No purchase confirmation

5

Asset purchase order

5

Asset sale order



2

Purchase of liquid securities

4

Transfer of liquid securities to cash

Result

- 1) Change of the UBO via the Fund
- 2) Transfer of \$ outside Russia

Asset – listed illiquid corporate bond, market value

Market price – 72 RUB./per asset



Monitoring risk transactions of an electronic wallet, process automation and algorithmization

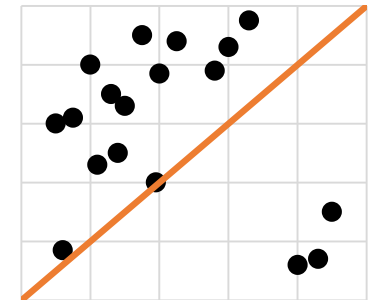
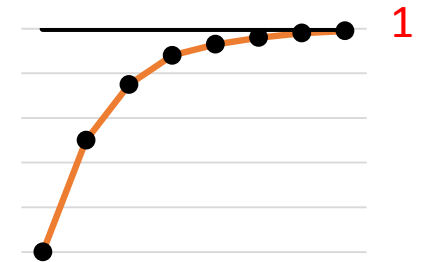
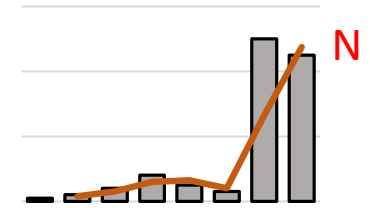
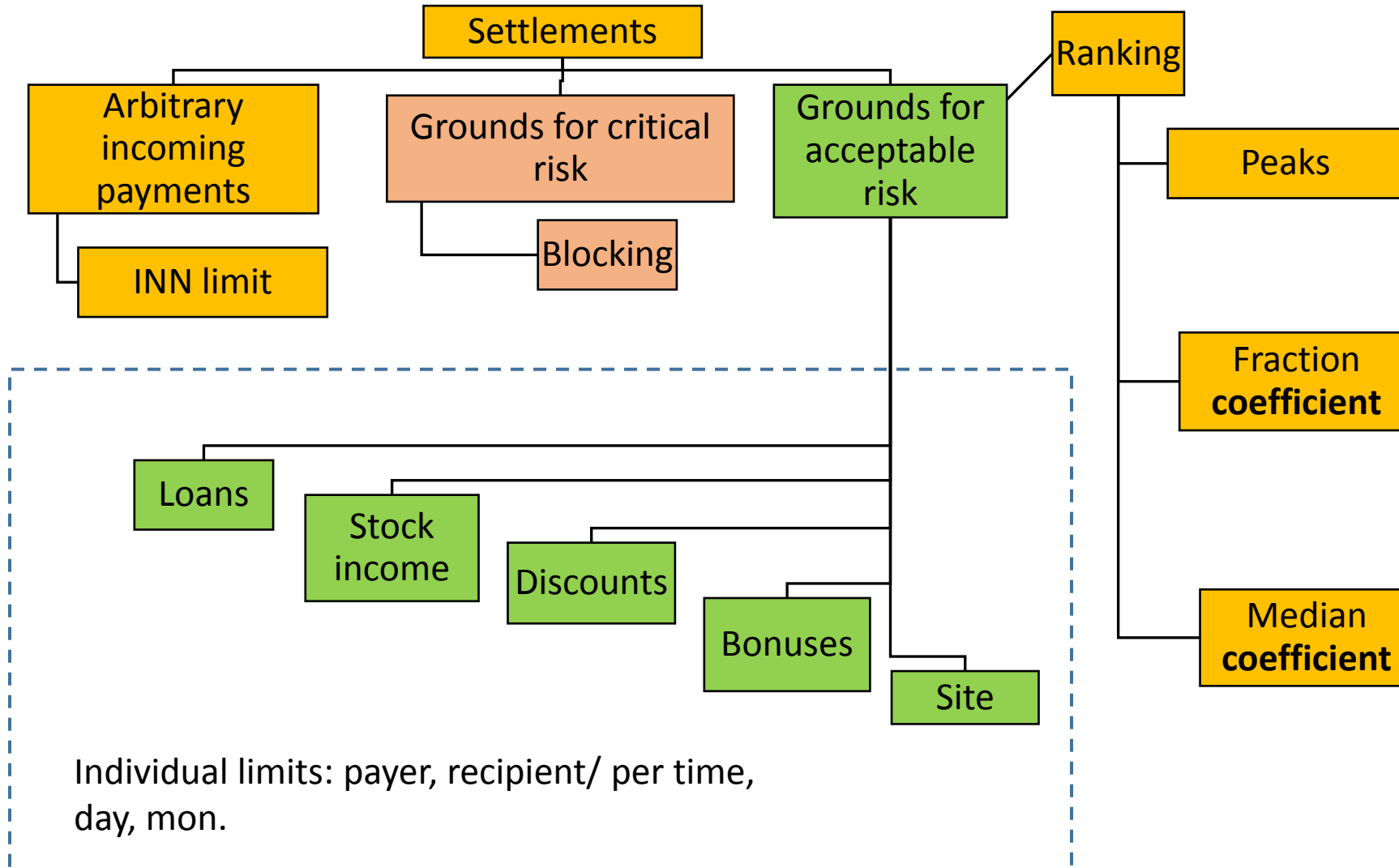
Dmitriy Gronin,

Head of the internal control service

Vasiliy Sergatskov,

Head of the information security and fraud prevention department

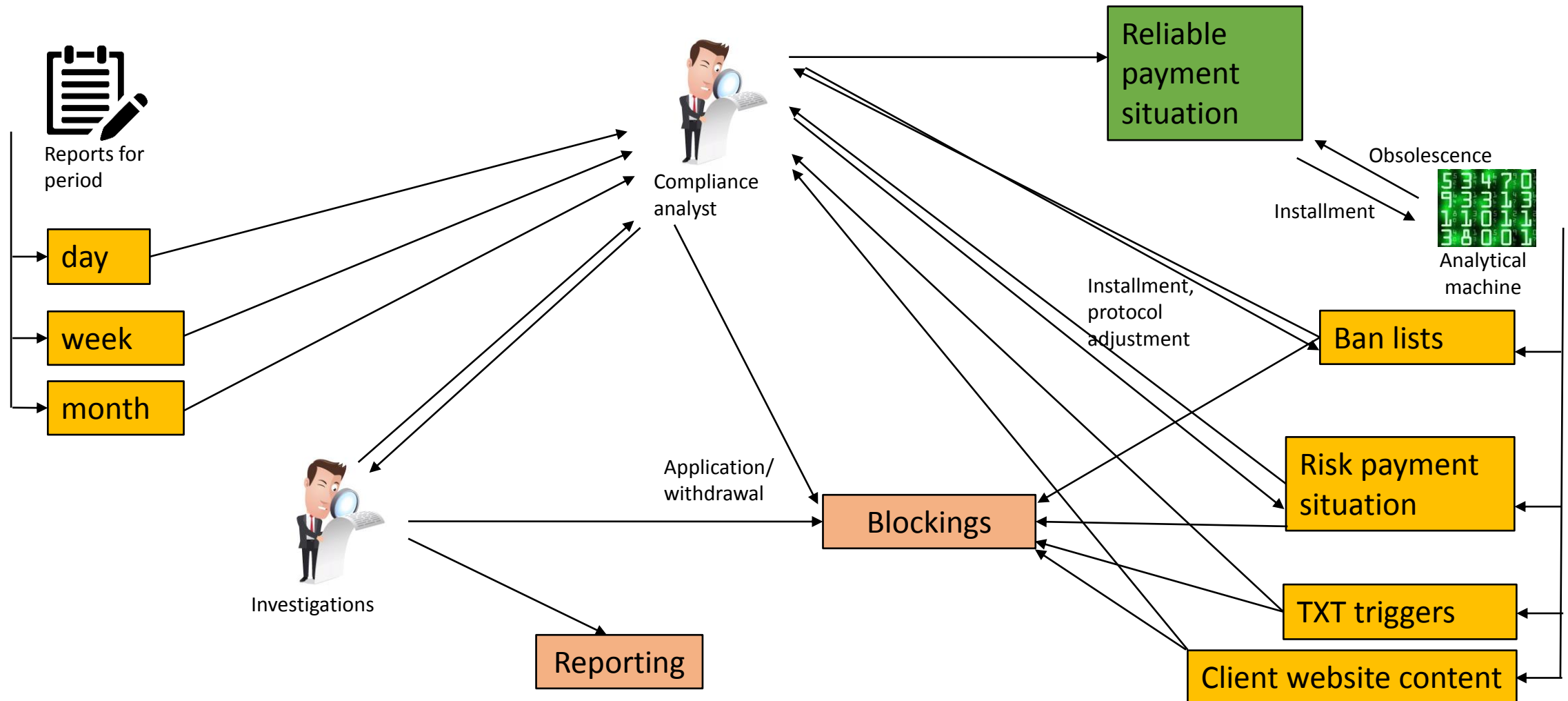
Managing the incoming flows of electronic money



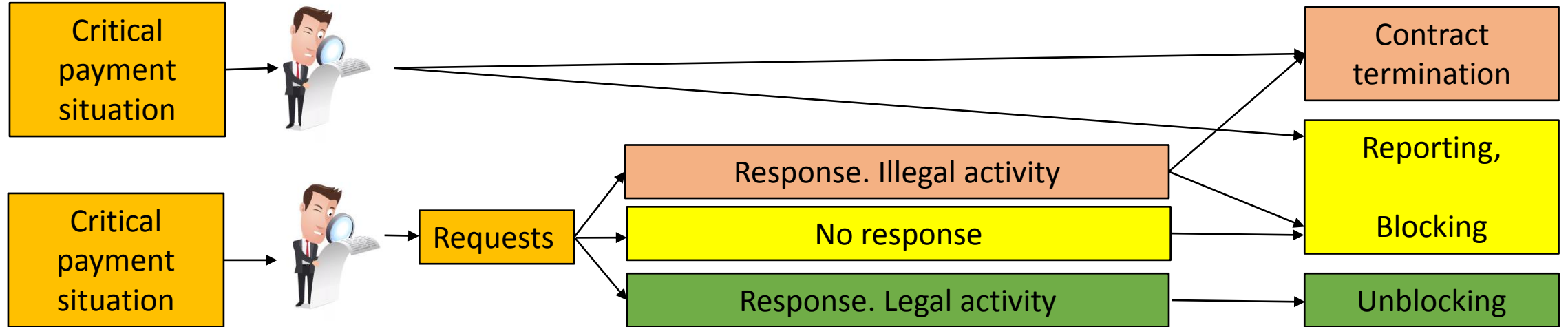
Indicators for periodic monitoring

- **Peaks**: weight of N biggest unique recipient's properties in the whole sum of payouts. It indicates if the biggest prominent recipients are exist.
- **Fraction coefficient**: the whole sum of payouts – to – number of recipient's properties and property limit ratio. Approximation of this coefficient to the “one” bellow shows that the real sums of payouts are consolidating themselves in the established limit's area.
- **Median coefficient**: weight of such biggest unique recipient's properties in the whole sum of payouts, that cover 50% of total payouts. This is an indicator of the payout's irregularity.

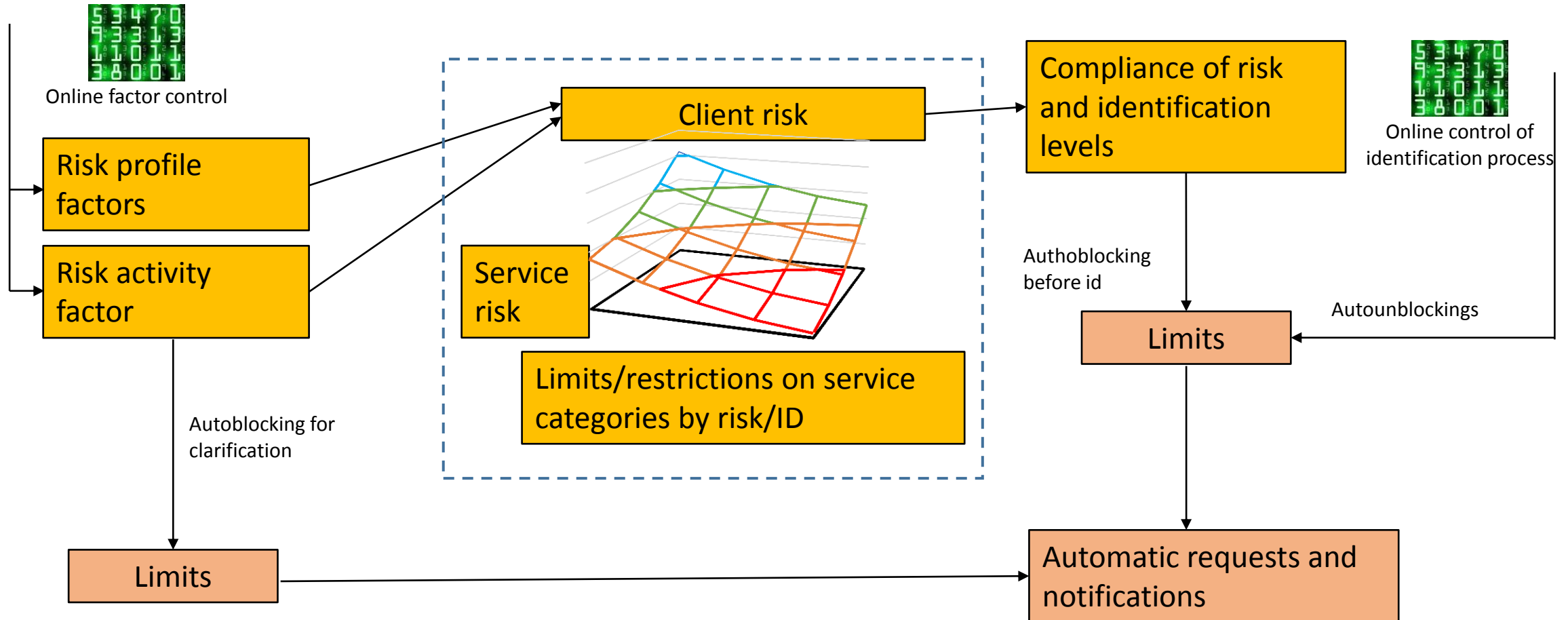
Managing the outgoing flows of electronic money



Investigation and reporting



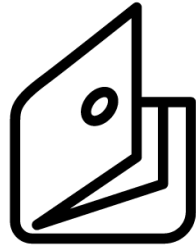
Risk and client identification management



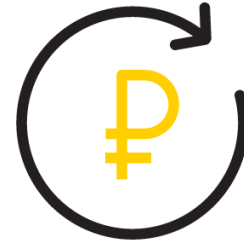
Payment types



Bank cards



E-money



Recurrent payments



Direct carrier
billing



QR-code



mPOS



ApplePay,
SamsungPay etc...
and more to come

Global overlap



devices

digital identities

payment tools

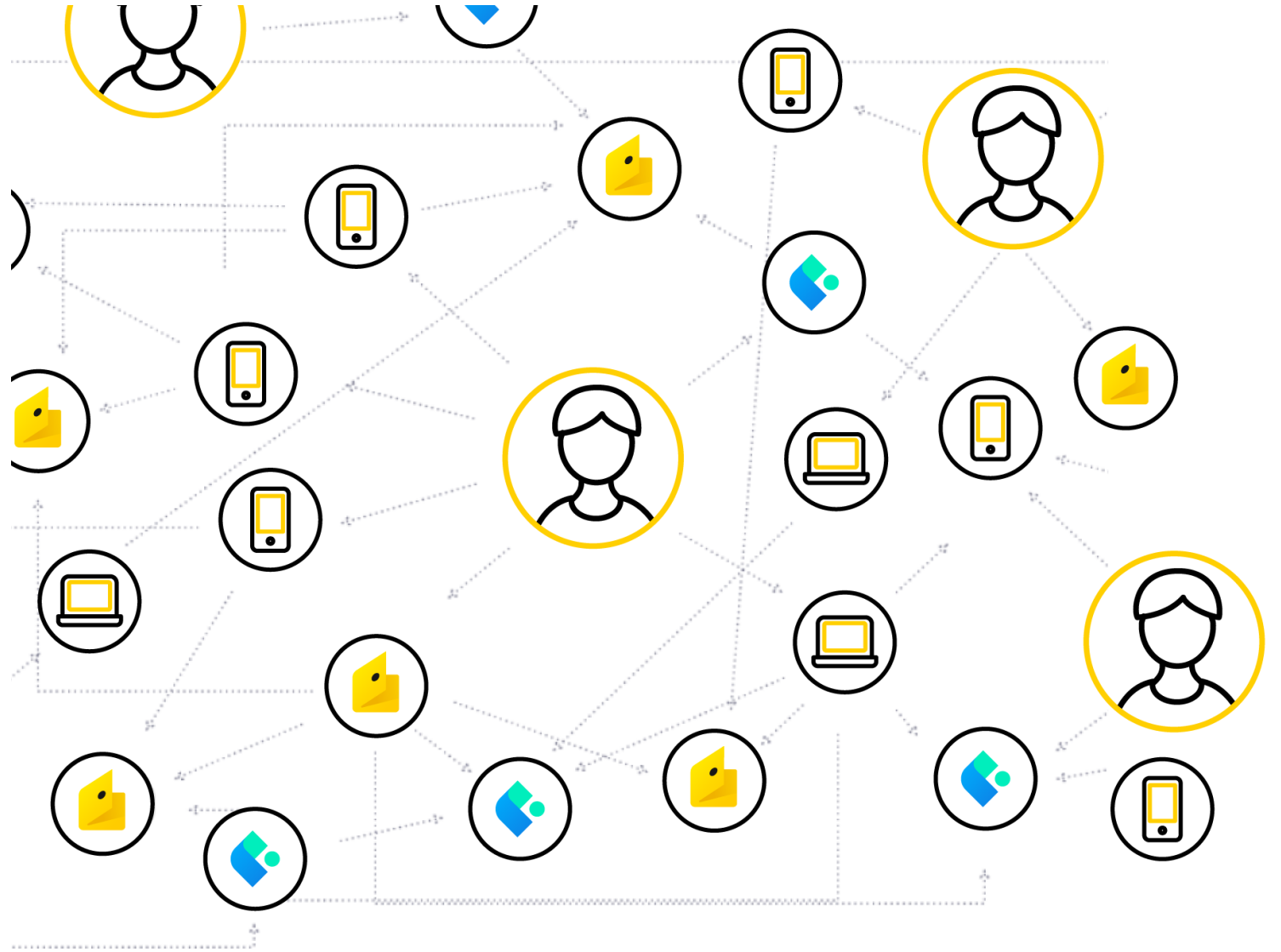
geo-location

emails

phones





IPs

...







Deep Learning vs Machine Learning

DL

-  Finds difficult dependences
-  Works with consequences
-  Needs a lot of data
-  Black box

ML

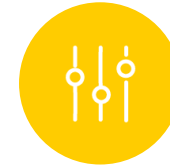
-  Rapid training process
-  Understandable models
-  Difficult features that been built by very qualified Data Engineer
-  Unable to find deep dependencies in data

The general approach



The task that will be decided with ML

Generate features is the most difficult and interesting part



Labeling data

Classification model and training process



Testing model and training again

Apply model



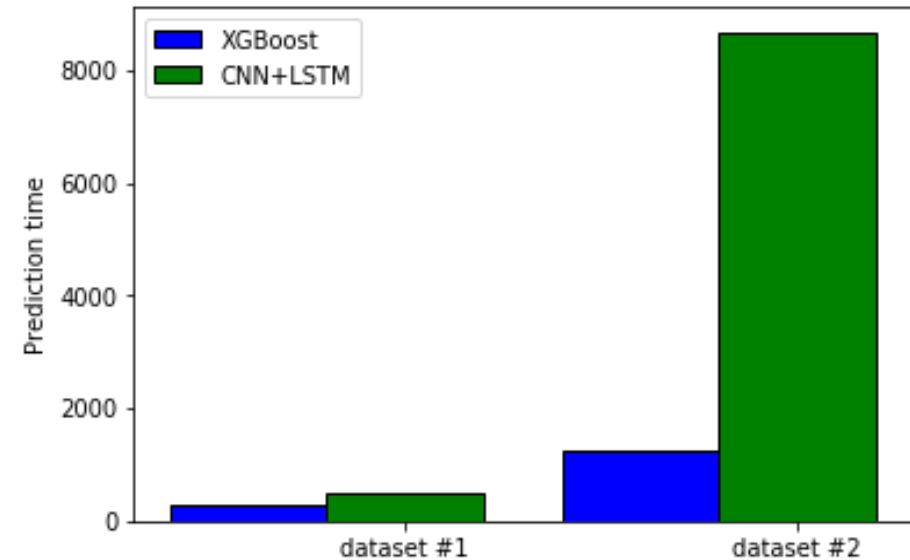
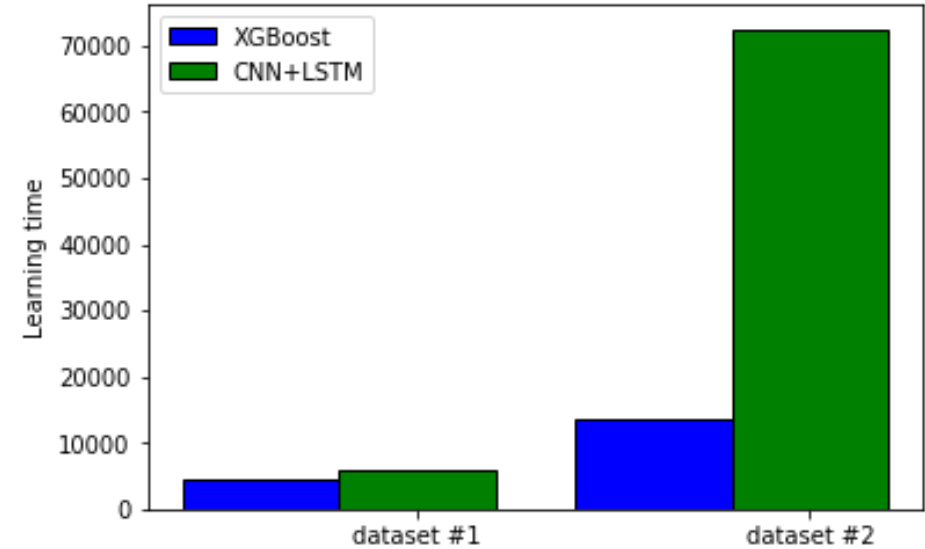
Features and predictions

-Dataset #1

Payment data: 54 features, 522 910 objects

-Dataset #2

Payment data + device data: 2 000 features, 522 910 objects (20/80)



Precision

Fraction of retrieved accounts that are relevant to the query

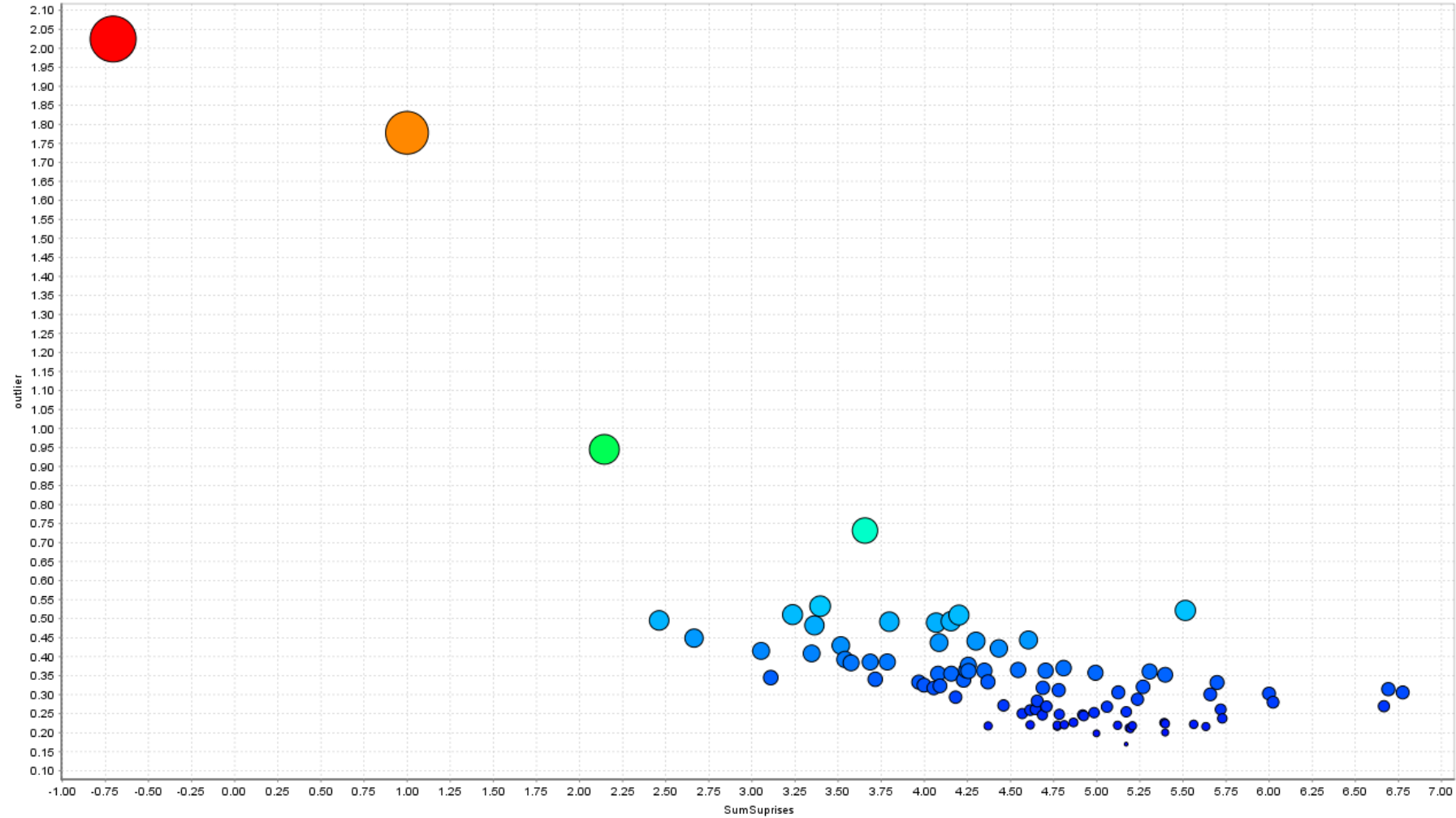
Metric: Precision	XGBoost	LSTM+CNN
Dataset #1	0.90795	0.94771
Dataset #2	0.91281	0.95831

Recall

Fraction of the relevant accounts that are successfully retrieved

Metric: Recall	XGBoost	LSTM+CNN
Dataset #1	0.96604	0.97891
Dataset #2	0.97234	0.98332

Customer anomaly detection



Lessons learned

Machine learning can't replace static rules and analysts.

Simple understandable models works very well only with supervising specialist knowing very well the subject.

Anomaly detection isn't a silver bullet, but sometimes it works!

Ак Барс
Банк



27.09.2019

Sergey Meshalkin (Ak Bars Bank Chief
Compliance Officer)

**Quality identification
as an instrument to prevent
illegal transactions**

Ak Bars Bank within the AML/CFT system

We are present in **27 regions of the country**, our headquarters being in Kazan.

We are the largest regional universal bank with the public ownership on the Republic of Tatarstan.

We hold **all types** of banking licenses existing in the Russian Federation.

We service **more than 4.3 Mio individuals and more than 50,000 corporate customers.**

We are among significant credit institutions in the market of payment services of Russia.

We are the member of the joint pilot project of the Central Bank and the Rosfinmonitoring to identify indicators of the terrorism financing.

We provide **more than 100 types of banking services** to corporate and private clients.

Member of the Compliance Council, holder of many commendations and letters of recognition by the Bank of Russia and Rosfinmonitoring for the contribution in the AML/CFT

The Bank, as a financial entity, faces the primary objective to efficiently apply measures for the combat of the money laundering, terrorism financing, and financing of the proliferation of weapons of mass destruction.

The properly organized work in terms of the identification of the customers, their representatives, and beneficiary owners is, in the Bank's opinion, one of the most critical aspects in the development of an efficient systems for combating the money laundering and terrorism financing.

Identification of the beneficiary owners and the relevant problematic issues

Ак Барс
Банк



An individual that directly or indirectly owns **the minimum percentage of a share of property** of the legal entity

An individual **controlling** the entity without the ownership due to participation in the financing of the entity

An individual **controlling** the legal entity in other ways: personal contacts with the persons in charge

An individual **responsible for making strategic decisions** that affect the development in a decisive manner

An individual **controlling** the day-to-day or regular activities of the legal entity **as an executive** using a position of a senior manager

The approach considering **the prevailing majority of shares**. Shareholders performing the control **solely** or jointly with other shareholders, including any contract, arrangement, relationship, mediator relations.

Problematic issues:

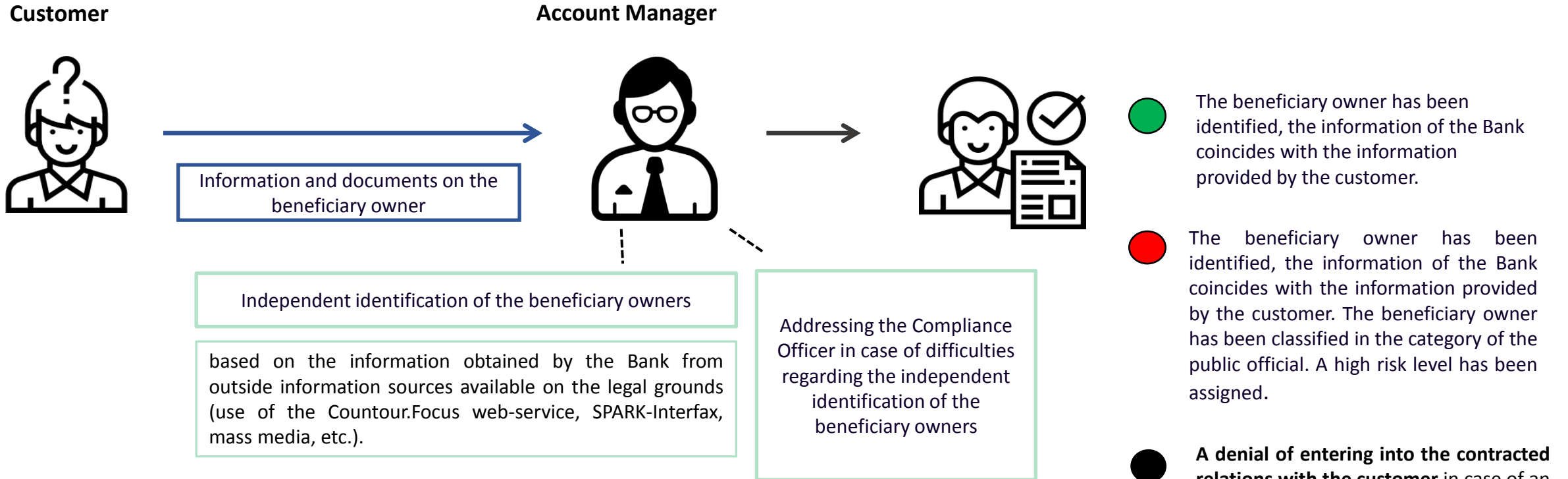
The information on the beneficiary owners may not be mentioned in the document of the companies, or their official involvement may be understated.

A problem of identification of beneficiary owners in trusts or holding structures

Non-disclosure of the information on the beneficiaries when using offshore structures to optimize the taxation or to avoid paying taxes, and in case of money laundering

All manners of documenting the property and drafting statutory documents are used for the purpose of the maximum concealment of the information on the personality of the beneficiary owner.

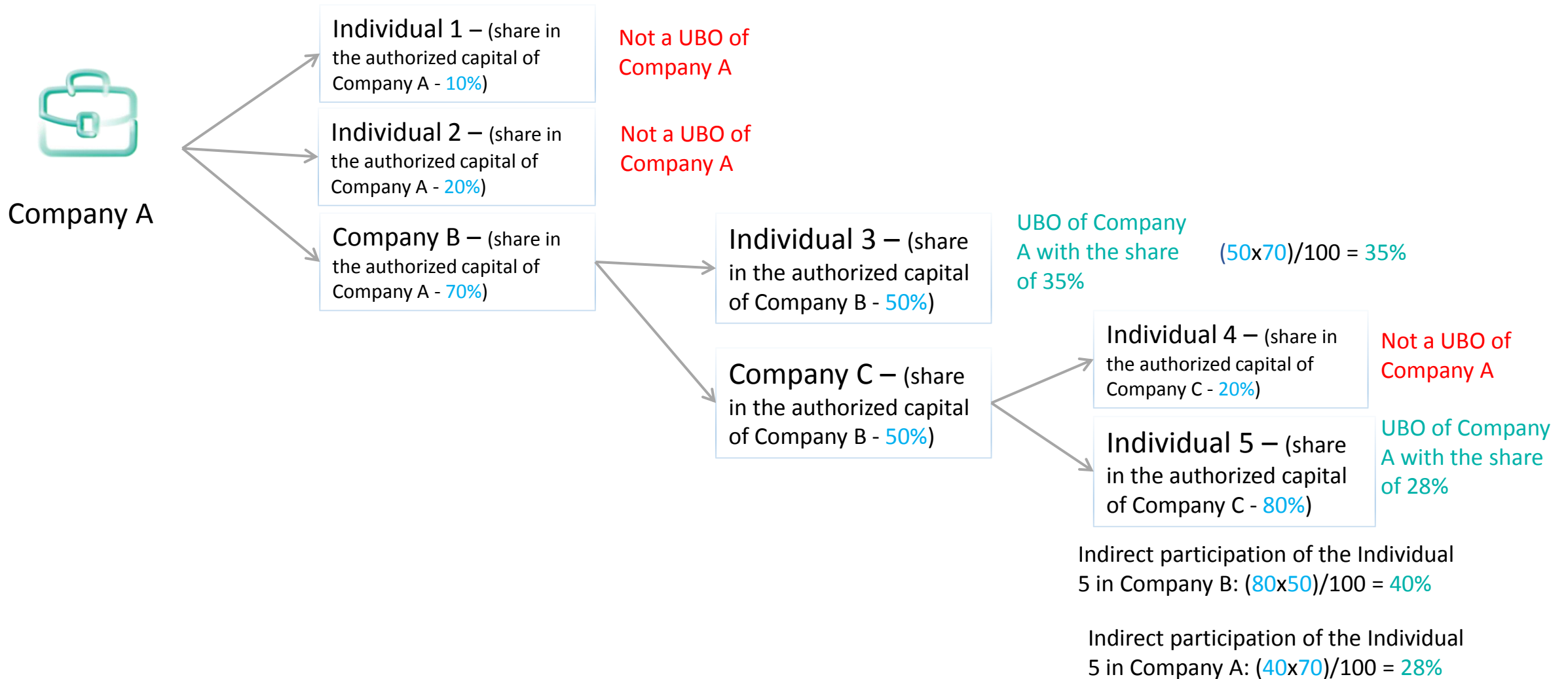
Measures taken by the Bank to identify owners of the business



Case:

The Bank reviewed an application of a legal entity M to open a settlement account. The customer provided the information on the individual beneficiary owner being the sole founder of the company. By analyzing the delivered documents and the information obtained from outside sources, the Bank came to a conclusion that the actual owner of the business is another individual different from that stated by the customer. Moreover, the legal entity featured signs of a fly-by-night company, and the founder of the company was a founder of 7 other legal entities. The customer was denied the acceptance for the servicing due to a lack of transparency regarding the end owners of the company and the suspicion of illegal activities performed by the controlled legal entities. The case was further reported regarding the denial for entering into the contracted relations.

Identification of the ultimate beneficiary owner using the cascade method



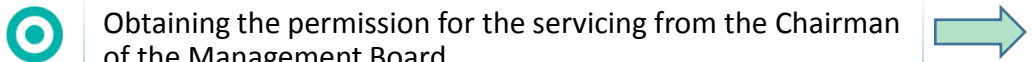
Management of risks of ML/TF when servicing persons related to PEPs



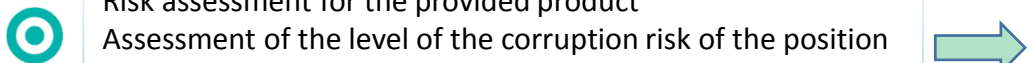
Identification of the fact of being within the surrounding of an international PEP when identifying the customer, determination of the degree of relations

Verification of the obtained information using the X-compliance service (Interfax)*

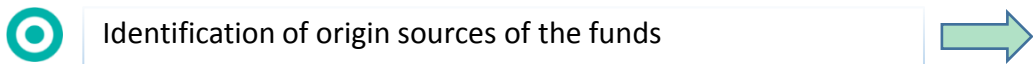
Filling in of a questionnaire of an established form by the customer



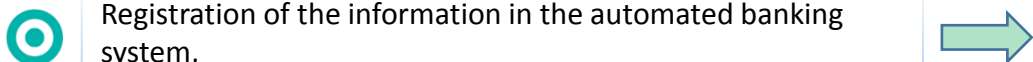
Obtaining the permission for the servicing from the Chairman of the Management Board



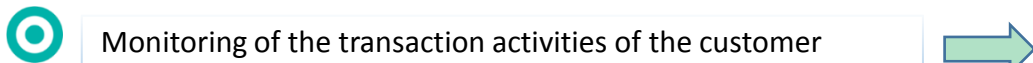
Risk assessment for the provided product
Assessment of the level of the corruption risk of the position of the PEP
Obtaining the information from open sources



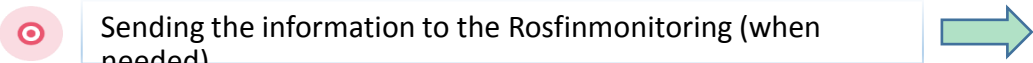
Identification of origin sources of the funds



Registration of the information in the automated banking system,
Assignment of the high level of risk



Monitoring of the transaction activities of the customer



Sending the information to the Rosfinmonitoring (when needed)

Физическое лицо				
Журавская Екатерина Всеволодна				
Категория: Близкое окружение МПДЛ, Близкое окружение	ID записи: 894831	Даты рождения: 1972-08-16 (,);	Дата смерти:	Пол: Женский
				Дата обновления: 14.06.2019
Документы Адреса Альтернативные наименования <u>Связанные лица</u> Списки наблюдения Санкционные ограничения Доп. информация Биография				
ФИО	Тип связи		Дата обновления	ID св. лица
Гуриев Сергей Маратович	супруг		2019-08-12 21:53:39	894829
Гуриев Марат Аликович	родитель супруга/супруги ребенка		2019-08-12 21:53:39	894830

*Example of the interface of the search engine

✓ *Permission obtained*

*A high-risk product – opening of an account with depositing the funds for the purpose of transfer of the funds abroad.
No adverse information has been found.*

Источник происхождения денежных средств:

личные сбережения ▼

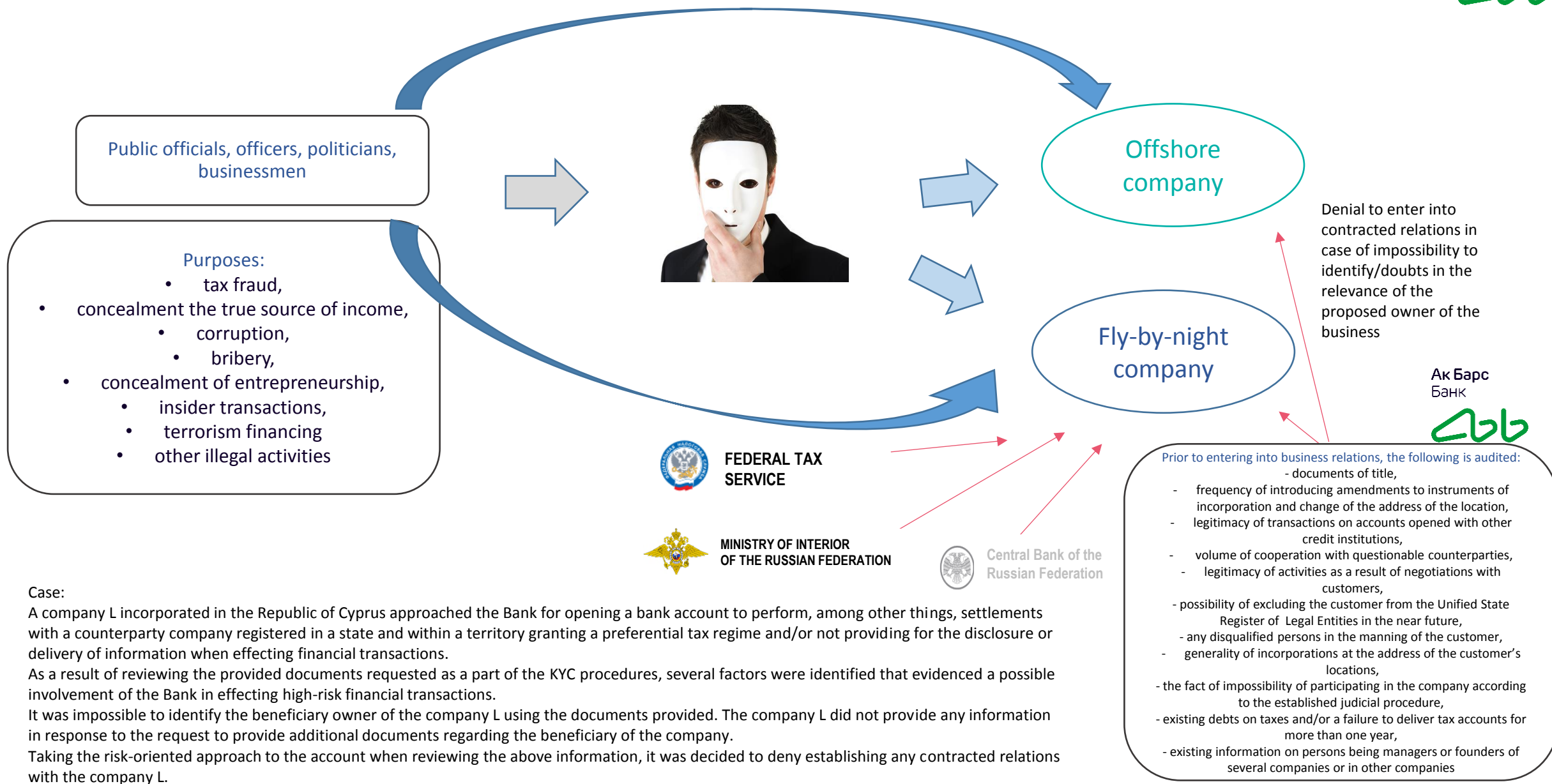
Уровень риска:

Высокий ▼

Daily automated account on the customer's transactions

A report in the form of an electronic message was sent with the code 6001 (1130) and a statement in the DESCR field that an account of a close relative of an international public official was cashed with a large sum of money that was later transferred to their account in a foreign credit institution.

Frontiers as an instrument of concealing information on actual beneficiaries



Case:

A company L incorporated in the Republic of Cyprus approached the Bank for opening a bank account to perform, among other things, settlements with a counterparty company registered in a state and within a territory granting a preferential tax regime and/or not providing for the disclosure or delivery of information when effecting financial transactions.

As a result of reviewing the provided documents requested as a part of the KYC procedures, several factors were identified that evidenced a possible involvement of the Bank in effecting high-risk financial transactions.

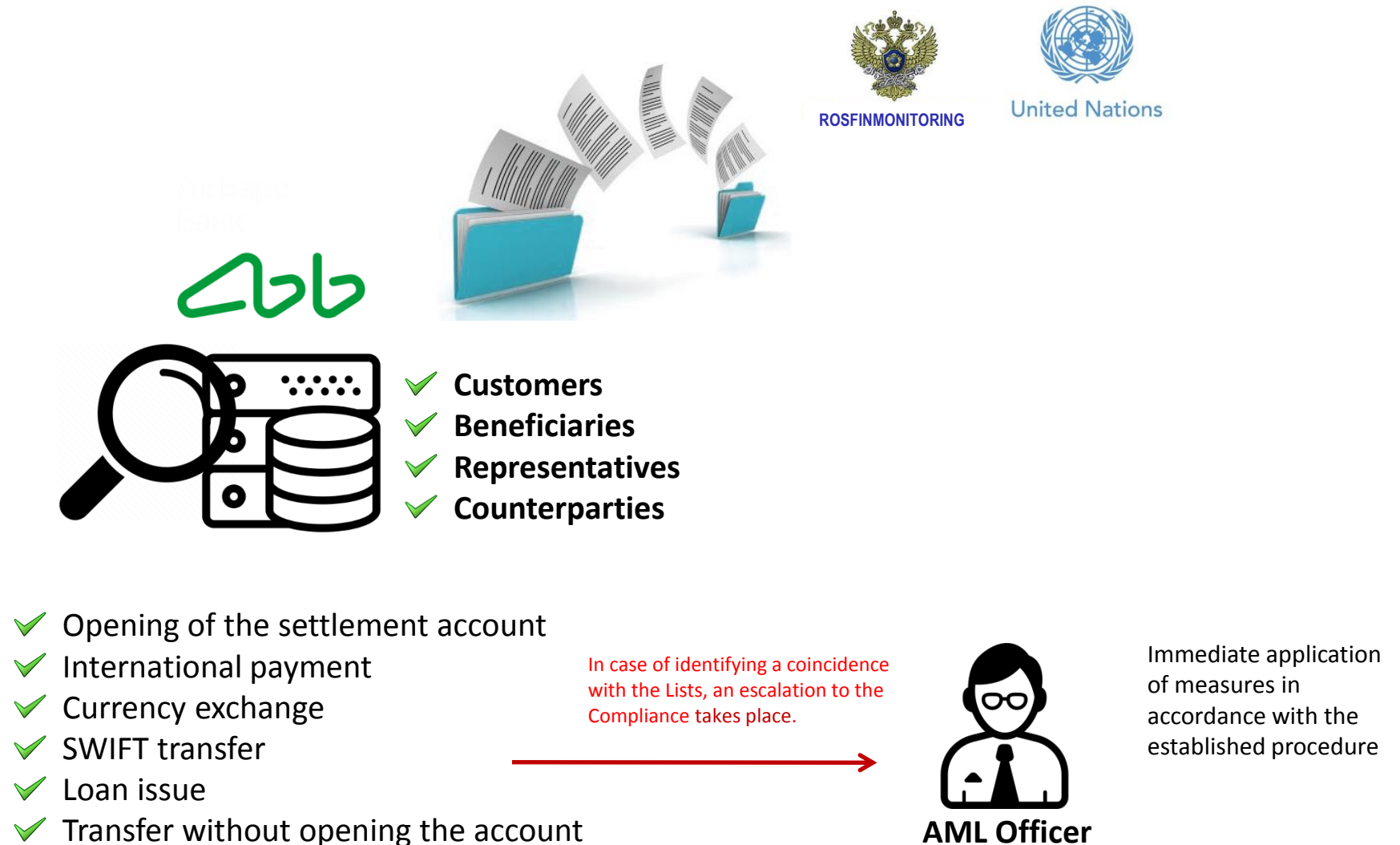
It was impossible to identify the beneficiary owner of the company L using the documents provided. The company L did not provide any information in response to the request to provide additional documents regarding the beneficiary of the company.

Taking the risk-oriented approach to the account when reviewing the above information, it was decided to deny establishing any contracted relations with the company L.

Mechanisms of identifying persons involved in extremisms or financing of proliferation of weapons of mass destruction by the Bank

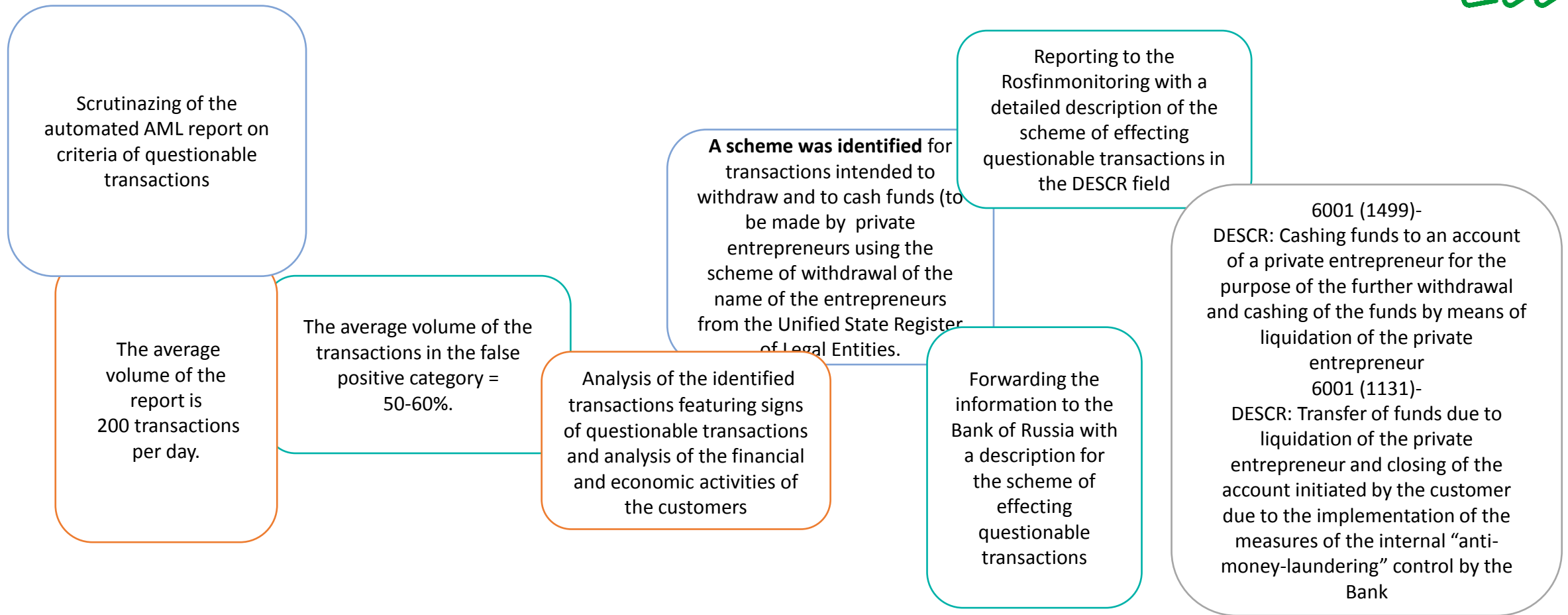
- Timely receipt of the list and their update in the automated banking system

- Audit of customers and affiliated persons, including their operations and transactions*



* An approximate list of the operations is given here.

Identification of new typologies of illegal activities of customers



Ак Барс
Банк



www.akbars.ru

Use of Device Fingerprinting to Identify Suspicious Customer Transactions and Activity

2019

Objectives. Identification of Vulnerabilities

Key objective – new approaches to the identification of suspicious customer transactions and activity in high-risk areas.

Main vulnerabilities:

- the use of shell companies;
- the ability to transfer criminal proceeds while concealing the identity of ultimate beneficiaries of criminal schemes behind nominee founders and directors;
- the use of online banking to manage company accounts.

Objectives. Identification of Vulnerabilities

The public and financial sectors are particularly vulnerable to criminal abuse, including by corrupt officials.

Funds are embezzled and laundered through a string of controlled shell companies.

The majority of illicit schemes to siphon off capital overseas and convert funds into cash are typically preceded by transactions involving pass-through accounts.

Steps Taken to Mitigate Risks

Focusing on typologies and ML schemes involving shell companies.

Adoption of measures to combat shell companies, including through the use of the mechanisms designed to prevent the registration of such companies to nominees.

Shell companies strive to mimic legitimate businesses.

Steps Taken to Mitigate Risks

As part of internal control procedures to manage the ML risks, among the factors affecting the customer risk assessment in the "customer and/or beneficial owner type-related risk" category is:

- a match between the identifier of the customer's device used to access the automated system and software required to transfer funds and the identifiers of devices of other customers, including those whose transactions were classified as suspicious.

Measures Adopted: IP Addresses

IP addresses – the accuracy and, as a result, value of information is not high enough, particularly where the identification of suspicious customer activity and transactions is automated.

Experience shows that the data is "littered" with matches.

13.09.2019	13:04:18	95.16	126
13.09.2019	13:05:38	95.16	126
13.09.2019	16:30:38	95.16	126
11.09.2019	17:59:22	217.6	217
09.09.2019	18:24:30		
06.09.2019	17:41:24		
06.09.2019	17:43:11		
05.09.2019	14:28:49		
03.09.2019	13:05:06		
30.08.2019	18:06:59		
30.08.2019	02:01:30	95.16	26
29.08.2019	00:15:53	217.6	80
26.08.2019	19:48:11	95.16	26
23.08.2019	14:37:39	95.16	26
22.08.2019	08:04:14	95.16	26

Количество связанных клиентов по видам связи			
Наименование клиента	Рег. номер к...		IP-адреса
		3	78
		3	78

Measures Adopted: Device Fingerprinting

Device (browser) fingerprinting allows a more accurate identification of suspicious customer transactions and activity.

Device fingerprints can be used to identify the user and his devices (by assigning an identifier) with the help of various indicators and characteristics.



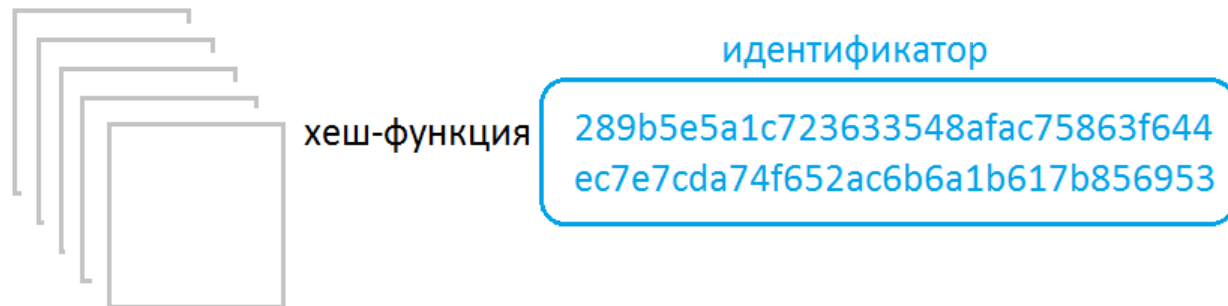
Measures Adopted: Device Fingerprinting

Examples of data types and indicators used to build a device identifier.

Data type	Description
Browser	End-user's browser details: type, name, version, supported languages, installed plug-ins, etc.
Fonts	Names of fonts installed on the end-user's computer.
Screen	Information related to the user's screen. Monitor resolution, workspace resolution, monitor color depth, etc.

The data array attributable to each device will almost always differ.

The data is transferred using a hash function and the output is a string of a fixed length, consisting of letters and numbers – the identifier.



Device Fingerprinting as a Tool

Device fingerprinting is not the sole objective, as it must be supported by rationale.

Elements of a model used to implement the risk management program:

- anomalies – one user with many devices or many users with one device;
- matches the devices of users whose transactions were classified as suspicious;
- maintaining a stop list of identifiers (processing rules) in order to use predictive analytics in respect of customer activity, including as an element of an on-line control system.

Device Fingerprinting as a Tool (examples)

Anomalies – one user with many devices or many users with one device.

One user with many devices

ID	Дата входа	Время в	IP-а	Hash	Тайм зона
1398697331	17.07.2019	16:43:25	94.2	32eb079dc91385f8dc4cdfdbe0924580ed82aeb80a6663d8a9c6d06602e7db2d	UTC+03:00
1398697331	22.07.2019	16:22:05	94.2	fe12ba83710 added90a899d2fc0d6acf6d97856bb1bef63bc43d30dca105ddbccc4	UTC+03:00
1398697331	01.08.2019	10:59:41	83.2	615cb32693f2e90177aa3ee4812cf83ae9ed83150b0dbec892499388dd806017	UTC+03:00
1398697331	22.08.2019	10:13:28	185	9f48137f316a6fdb6db8d38f0fa20de3e1cf9527c3a8678b0f3c30fbcf301dd5	UTC+03:00
1398697331	22.08.2019	13:02:15	185	9bd7af56123dcdf2c9dcb6eb34d30575dd986448f7090d127ef0a886429d05ab	UTC+03:00
1398697331	22.08.2019	15:42:20	185	a94bb1089b24ebd782811aa41f71bc92daa3c076936a29fccd933021649c1e22	UTC+03:00
1398697331	22.08.2019	15:55:16	185	d561de9b1f3456cd90977ca0bf053f1fc64ffda8c97e14a742774e8a1020bba5	UTC+03:00
1398697331	22.08.2019	16:17:33	185	a7c34b7146b6aa449137e111db64e7d4b463a010b8a007c6f95ab0808aec671b	UTC+03:00
1398697331	22.08.2019	18:13:50	185	243597df652c184407130e1b050996450abc5f6628641128c7c54b222305c4a	UTC+03:00

The use by the user of the browser (built-in emulators, “incognito mode”, etc.) or third-party utilities (software) that change any browser settings randomly.

Device Fingerprinting as a Tool (examples)

Anomalies – one user with many devices or many users with one device.

Many users with one device

ID	Дата входа	Время входа	IP-адрес	Hash	Тайм зона
1375579473	20.09.2019	18:23:35	95.	289b5e5a1c723633548afac75863f644ec7e7cda74f652ac6b6a1b617b856953	UTC+03:00
1326013649	20.09.2019	18:19:30	95.	289b5e5a1c723633548afac75863f644ec7e7cda74f652ac6b6a1b617b856953	UTC+03:00
1389117974	20.09.2019	18:10:01	95.	289b5e5a1c723633548afac75863f644ec7e7cda74f652ac6b6a1b617b856953	UTC+03:00
1396117101	20.09.2019	18:07:35	95.	289b5e5a1c723633548afac75863f644ec7e7cda74f652ac6b6a1b617b856953	UTC+03:00
1354881404	20.09.2019	18:07:05	95.	289b5e5a1c723633548afac75863f644ec7e7cda74f652ac6b6a1b617b856953	UTC+03:00
1390181672	20.09.2019	17:57:34	95.	289b5e5a1c723633548afac75863f644ec7e7cda74f652ac6b6a1b617b856953	UTC+03:00
1389117974	20.09.2019	17:57:27	95.	289b5e5a1c723633548afac75863f644ec7e7cda74f652ac6b6a1b617b856953	UTC+03:00
1390181672	20.09.2019	16:24:46	217	289b5e5a1c723633548afac75863f644ec7e7cda74f652ac6b6a1b617b856953	UTC+03:00
1389117974	20.09.2019	16:21:52	217	289b5e5a1c723633548afac75863f644ec7e7cda74f652ac6b6a1b617b856953	UTC+03:00
1392080980	20.09.2019	11:15:02	95.	289b5e5a1c723633548afac75863f644ec7e7cda74f652ac6b6a1b617b856953	UTC+03:00

Device Fingerprinting as a Tool (examples)

Matches the devices of users whose transactions were classified as suspicious.

ID	Дата входа	Время входа	IP-адрес	Hash	Тайм зона
1375579473	20.09.2019	18:23:35	95.	289b5e5a1c723633548afac75863f644ec7e7cda74f652ac6b6a1b617b856953	UTC+03:00
1326013649	20.09.2019	18:19:30	95.	289b5e5a1c723633548afac75863f644ec7e7cda74f652ac6b6a1b617b856953	UTC+03:00
1389117974	20.09.2019	18:10:01	95.	289b5e5a1c723633548afac75863f644ec7e7cda74f652ac6b6a1b617b856953	UTC+03:00
1396117101	20.09.2019	18:07:35	95.	289b5e5a1c723633548afac75863f644ec7e7cda74f652ac6b6a1b617b856953	UTC+03:00
1354881404	20.09.2019	18:07:05	95.	289b5e5a1c723633548afac75863f644ec7e7cda74f652ac6b6a1b617b856953	UTC+03:00
1390181672	20.09.2019	17:57:34	95.	289b5e5a1c723633548afac75863f644ec7e7cda74f652ac6b6a1b617b856953	UTC+03:00
1389117974	20.09.2019	17:57:27	95.	289b5e5a1c723633548afac75863f644ec7e7cda74f652ac6b6a1b617b856953	UTC+03:00
1390181672	20.09.2019	16:24:46	217.	289b5e5a1c723633548afac75863f644ec7e7cda74f652ac6b6a1b617b856953	UTC+03:00
1389117974	20.09.2019	16:21:52	217.	289b5e5a1c723633548afac75863f644ec7e7cda74f652ac6b6a1b617b856953	UTC+03:00
1392080980	20.09.2019	11:15:02	95.	289b5e5a1c723633548afac75863f644ec7e7cda74f652ac6b6a1b617b856953	UTC+03:00

Стоп-лист

289b5e5a1c723633548afac75863f644ec7e7cda74f652ac6b6a1b617b856953
10912eb8fc868f9a268163c8e15c6529cc8f9dc405533bb51d133ed6f47fc6e6

ID	Дата входа	Время входа	IP-адрес	Имя устройства	Hash
1392080980	20.09.2019	11:15:02	95.	Windows 10 IE 11.0	289b5e5a1c723633548afac75863f644ec7e7cda74f652ac6b6a1b617b856953
1392080980	13.09.2019	13:04:18	95.	Windows 10 IE 11.0	289b5e5a1c723633548afac75863f644ec7e7cda74f652ac6b6a1b617b856953
1392080980	13.09.2019	16:30:38	95.	Windows 10 IE 11.0	289b5e5a1c723633548afac75863f644ec7e7cda74f652ac6b6a1b617b856953
1392080980	13.09.2019	13:05:38	95.	Windows 10 IE 11.0	289b5e5a1c723633548afac75863f644ec7e7cda74f652ac6b6a1b617b856953
1392080980	11.09.2019	17:59:22	217.	Windows 10 IE 11.0	289b5e5a1c723633548afac75863f644ec7e7cda74f652ac6b6a1b617b856953
1392080980	09.09.2019	18:24:30	217.	Windows 10 IE 11.0	289b5e5a1c723633548afac75863f644ec7e7cda74f652ac6b6a1b617b856953
1392080980	08.08.2019	17:22:48	176.	Mac OS X 10.13.6 Chrome 75.0.3770	10912eb8fc868f9a268163c8e15c6529cc8f9dc405533bb51d133ed6f47fc6e6
1392080980	16.07.2019	14:09:51	176.	Mac OS X 10.13.6 Chrome 75.0.3770	10912eb8fc868f9a268163c8e15c6529cc8f9dc405533bb51d133ed6f47fc6e6

Device Fingerprinting as a Tool (examples)

Maintaining a stop list of identifiers in order to use predictive analytics in respect of customer activity, including as an element of an on-line monitoring system.

ID	Дата входа	Время входа	IP-адрес	Имя устройства	Hash
1326013649	02.08.2019	18:13:20	95.1	Windows 10 IE 11.0	289b5e5a1c723633548afac75863f644ec7e7cda74f652ac6b6a1b617b856953
1326013649	30.07.2019	11:44:28	185	Windows 10 IE 11.0	289b5e5a1c723633548afac75863f644ec7e7cda74f652ac6b6a1b617b856953
1326013649	24.07.2019	12:29:54	185	Windows 10 IE 11.0	289b5e5a1c723633548afac75863f644ec7e7cda74f652ac6b6a1b617b856953
1326013649	24.07.2019	16:50:45	95.1	Windows 10 IE 11.0	289b5e5a1c723633548afac75863f644ec7e7cda74f652ac6b6a1b617b856953
1326013649	23.07.2019	14:23:09	185	Windows 10 IE 11.0	289b5e5a1c723633548afac75863f644ec7e7cda74f652ac6b6a1b617b856953
1326013649	18.07.2019	13:13:30	185	Windows 10 IE 11.0	289b5e5a1c723633548afac75863f644ec7e7cda74f652ac6b6a1b617b856953
1326013649	16.03.2019	10:27:38	37.1	Mac OS X 10.13.6 Chrome 72.0.3626	10912eb8fc868f9a268163c8e15c6529cc8f9dc405533bb51d133ed6f47fc6e6
1326013649	25.02.2019	11:11:32	78.1	Mac OS X 10.13.6 Chrome 71.0.3578	10912eb8fc868f9a268163c8e15c6529cc8f9dc405533bb51d133ed6f47fc6e6

ID	Дата входа	Время входа	IP-адрес	Имя устройства	Hash
1365766600	30.07.2019	12:26:16	185	Windows 10 IE 11.0	289b5e5a1c723633548afac75863f644ec7e7cda74f652ac6b6a1b617b856953
1365766600	29.07.2019	17:09:50	217	Windows 10 IE 11.0	289b5e5a1c723633548afac75863f644ec7e7cda74f652ac6b6a1b617b856953
1365766600	25.07.2019	14:45:06	95.1	Windows 10 IE 11.0	289b5e5a1c723633548afac75863f644ec7e7cda74f652ac6b6a1b617b856953
1365766600	23.07.2019	12:41:18	185	Windows 10 IE 11.0	289b5e5a1c723633548afac75863f644ec7e7cda74f652ac6b6a1b617b856953
1365766600	19.07.2019	13:27:53	185	Windows 10 IE 11.0	289b5e5a1c723633548afac75863f644ec7e7cda74f652ac6b6a1b617b856953
1365766600	27.05.2019	20:09:54	217	Mac OS X 10.13.6 Chrome 74.0.3729	10912eb8fc868f9a268163c8e15c6529cc8f9dc405533bb51d133ed6f47fc6e6

ID	Дата входа	Время входа	IP-адрес	Имя устройства	Hash
1392080980	20.09.2019	11:15:02	95.1	Windows 10 IE 11.0	289b5e5a1c723633548afac75863f644ec7e7cda74f652ac6b6a1b617b856953
1392080980	13.09.2019	13:04:18	95.1	Windows 10 IE 11.0	289b5e5a1c723633548afac75863f644ec7e7cda74f652ac6b6a1b617b856953
1392080980	13.09.2019	16:30:38	95.1	Windows 10 IE 11.0	289b5e5a1c723633548afac75863f644ec7e7cda74f652ac6b6a1b617b856953
1392080980	13.09.2019	13:05:38	95.1	Windows 10 IE 11.0	289b5e5a1c723633548afac75863f644ec7e7cda74f652ac6b6a1b617b856953
1392080980	11.09.2019	17:59:22	217	Windows 10 IE 11.0	289b5e5a1c723633548afac75863f644ec7e7cda74f652ac6b6a1b617b856953
1392080980	09.09.2019	18:24:30	217	Windows 10 IE 11.0	289b5e5a1c723633548afac75863f644ec7e7cda74f652ac6b6a1b617b856953
1392080980	08.08.2019	17:22:48	176	Mac OS X 10.13.6 Chrome 75.0.3770	10912eb8fc868f9a268163c8e15c6529cc8f9dc405533bb51d133ed6f47fc6e6
1392080980	16.07.2019	14:09:51	176	Mac OS X 10.13.6 Chrome 75.0.3770	10912eb8fc868f9a268163c8e15c6529cc8f9dc405533bb51d133ed6f47fc6e6

Device Fingerprinting – Conclusions

The integration by credit institutions of the device fingerprinting technology into their risk management strategies to identify suspicious customer transactions and activity (incl. to combat the use of shell companies):

- improves the accuracy and speed of identification of customers that are shell companies;
- improves the accuracy of identification of controlled shell companies (incl. from the “registrars” category);
- allows the use of predictive analytics in respect of customer activity;
- as a result, improves the quality of suspicious transactions reports (STRs);
- the on-line monitoring system is augmented with multiple scenarios (the use of a new initiating trigger).



Money Laundering, Terrorism Finance Risks Assessment in EBRD operations

EAG/ITMCF Workshop, Kazan, September 2019



European Bank
for Reconstruction and Development

Integrity Due Diligence Guidelines

The core document that outlines the acceptable integrity standards and principles that should underpin every integrity due diligence exercise.

IDD Guidelines provides that

Initial responsibility for risk assessment lies with the EBRD Banking team. Banking teams can best ensure that the Bank's objectives are achieved by adhering strictly to its integrity due diligence procedures which set out the respective roles of the Banking teams, Risk Management and OCCO.

Integrity Due Diligence Procedures

Supplement to the Guidelines that describes the steps to be completed by the Bank staff conducting integrity due diligence for all projects.

The document provides that

The Anti-Money Laundering and Counter-Terrorist Financing Checklist (“AML/CFT Checklist”) must be completed by Banking for all projects involving financial institutions or pooled vehicles in any capacity, reflecting the unique risks associated with such entities. Pooled vehicles include private equity funds, as well as any other entity in which capital contributions are pooled and invested.

AML/CFT Due Diligence Procedures

It describes the steps to be completed by Bank staff conducting integrity due diligence for all FI and pooled vehicle projects.

Banking team is required

- For Non-FI projects: Evaluate money laundering and terrorism financing risks as part of the Integrity Due Diligence Procedures.
- For all Financial Institution (FI) projects and all types of Pooled Vehicles (property/equity/investment funds): Complete Anti-Money Laundering and Counter-Terrorism Financing Checklist (the “AML/CFT Checklist”).

The document provides that

- ✓ The Bank will not proceed on a Project without knowing who the beneficial owner is.
- ✓ The Bank will not engage in a relationship with anyone convicted of, or under investigation for, a serious criminal offence.
- ✓ The Bank will not engage with anyone or any entity currently on an internationally recognized “Black List”.
- ✓ The Bank will not undertake Projects where there is credible evidence of existing links to organised crime and criminal activities.
- ✓ Relationships with PEPs, clients with poor past business practices or other high-risk clients and Projects in certain higher risk sectors require enhanced due diligence.

- ✓ International sanctions have expanded considerably in recent years and teams must be alert to the risks of Projects that could be impacted by sanctions.
- ✓ Tax avoidance/evasion and the use of offshore jurisdictions are getting intense scrutiny internationally and at the Board.
- ✓ Terrorist financing and money laundering are increasingly important issues and many businesses in our countries of operation are at risk. If a financial institution is involved in any Project, the team must complete the AML/CFT checklist.

The EBRD, via OCCO, has an observer status at FATF and EAG, regularly attends Plenary meetings and following their decisions undertakes appropriate measures to enhance its due diligence.

- ✓ FI and 'Funds' projects - mandatory to complete both IDD red flags checklist and AML/CTF checklist.
- ✓ Other projects – no need to complete separate AML/CTF checklist, only the IDD red flags checklist. However, be aware.
- ✓ Focus on the effectiveness of FI / Funds' controls, not simply apparent existence.
- ✓ Loan prepayments or from sources other than the borrower, refer to Operations Administration Dept.
- ✓ Any other doubts? Ask OCCO.

Client FI / funds Required Controls



European Bank
for Reconstruction and Development

- ✓ Customer Identification
- ✓ 'Know Your Customer / Context (KYC)'
- ✓ Enhanced scrutiny of higher risk customers such as PEPs and correspondent banks
- ✓ Account Monitoring and Suspicion Reporting
- ✓ Records maintenance / Staff training
- ✓ Use of international findings
- ✓ Appointment of Compliance Officers/MLROs
- ✓ Effectiveness



All relevant entities – Terrorist Financing

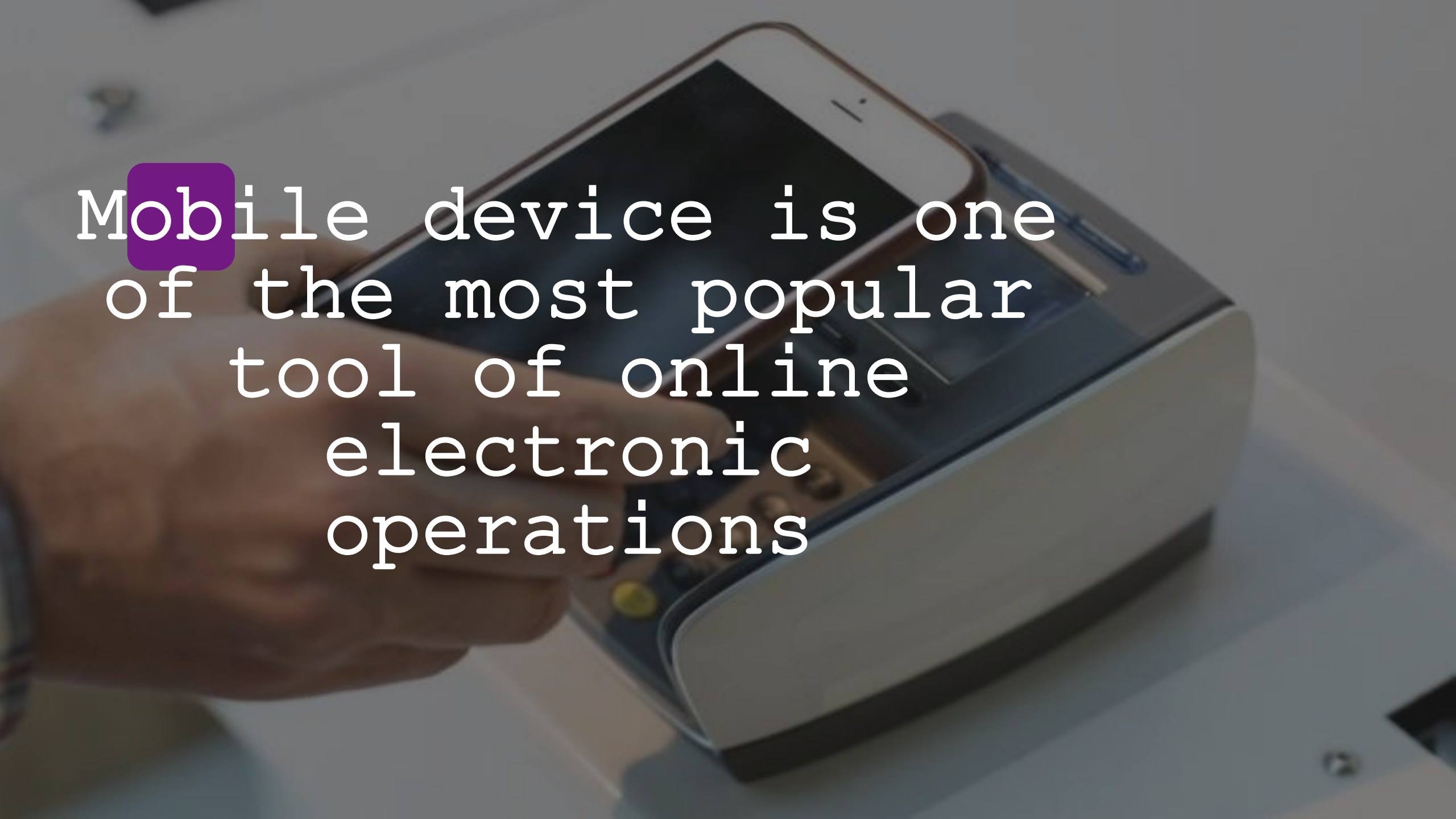
- ✓ UN Security Council Resolutions and FATF TF Recommendations
- ✓ Name-checking of names/activities against UN lists
- ✓ Prohibition of provision of financial services to those on UN lists



Risk. It isn't always
where you expect it to be.

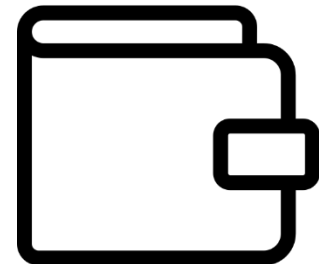
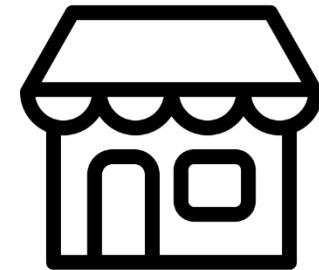
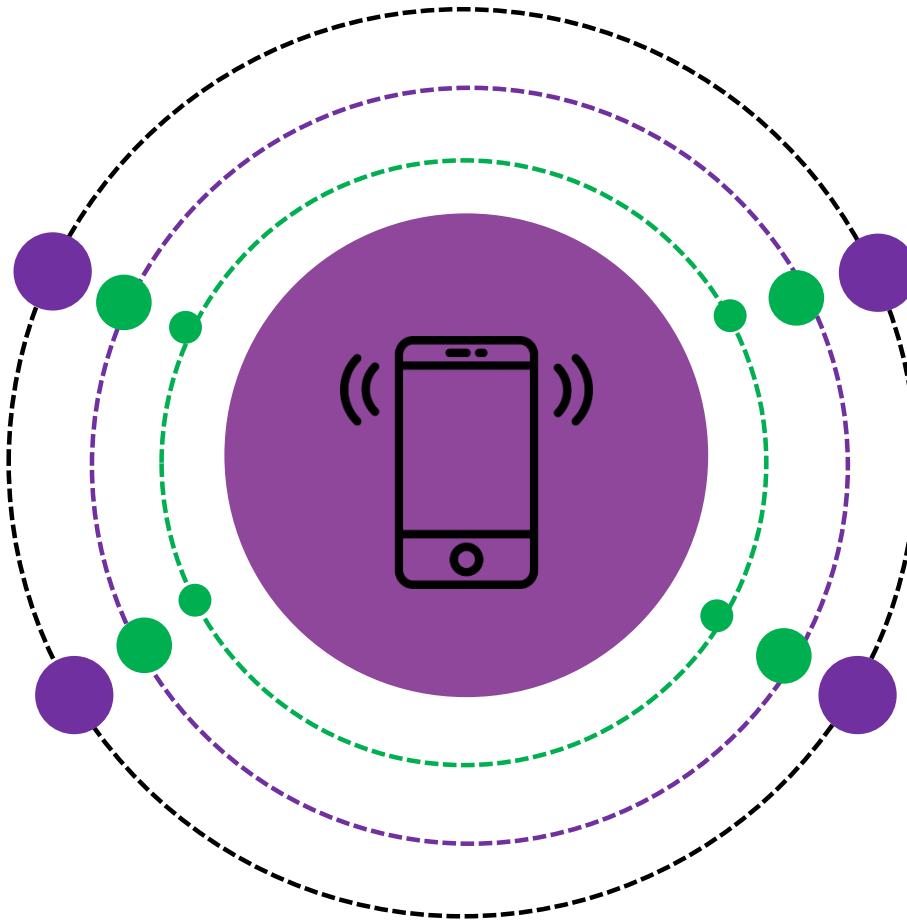
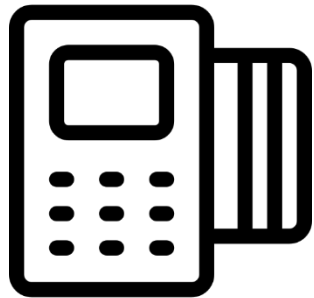
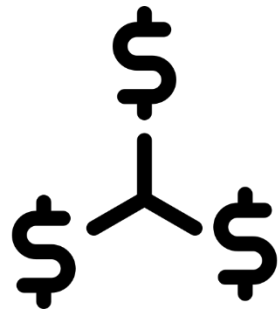
An aerial night photograph of a city, featuring a prominent, brightly lit skyscraper in the center. The surrounding urban landscape is visible with various other buildings and streets. The text is overlaid on the image, with the first letter 'F' highlighted in a green square.

Financial monitoring and identification of suspicious client activity by telecommunication companies

A hand is holding a smartphone over a payment terminal. The terminal has a screen and a keypad. The background is a light-colored surface.

Mobile device is one
of the most popular
tool of online
electronic
operations

Advantages of mobile phone provider





Mobility

Extensive service
network

Transmission
infrastructure

Product versatility for
operations conducting

What have you
to control
(monitor)?



Attention №1

For cash transactions : withdrawing or crediting cash money to the personal account of legal entity's





Attention №2

Crediting funds or debiting funds from a personal account of a legal entity, activity period doesn't exceed three months from the date of it's registration

The same actions, if operations were not conducting to the specified personal account since it was opened

Attention №3

Crediting funds or transferring cash to the personal accounts, if a member of operation has a registration, residence, location in Republic of Iran and DPRK country



Banking

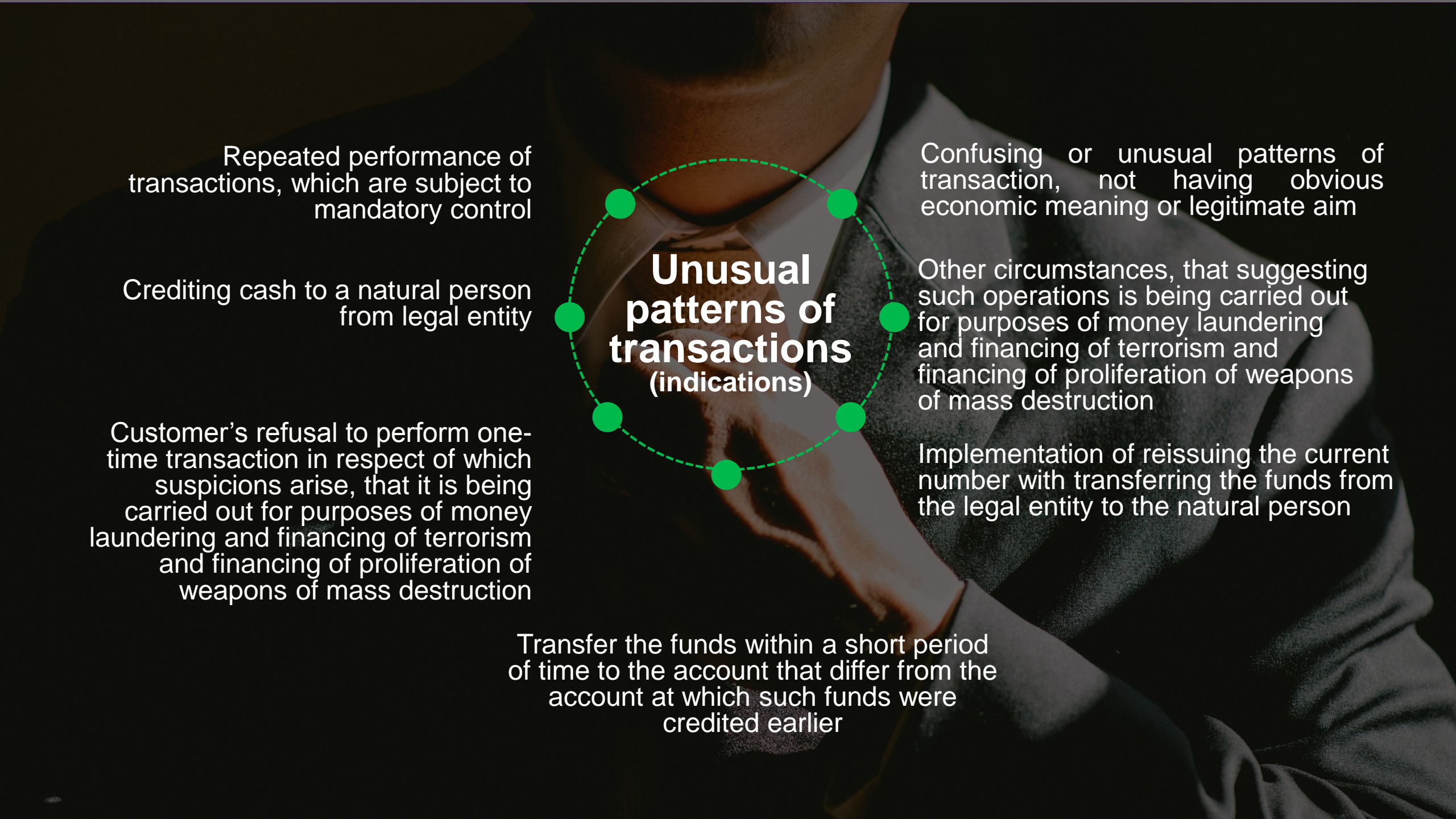
What else have you
to control
(monitor)?



Balance

Monthly

Annual

A person in a dark suit and tie is shown from the chest up. Overlaid on the image is a central diagram consisting of a dashed green circle with five solid green dots at its perimeter. Inside this circle, the text 'Unusual patterns of transactions (indications)' is written in white. Surrounding this central circle are six text blocks, each describing a specific indicator of unusual transaction patterns. The background is a dark, slightly blurred image of the person's face and suit.

Unusual patterns of transactions (indications)

Repeated performance of transactions, which are subject to mandatory control

Crediting cash to a natural person from legal entity

Customer's refusal to perform one-time transaction in respect of which suspicions arise, that it is being carried out for purposes of money laundering and financing of terrorism and financing of proliferation of weapons of mass destruction


Confusing or unusual patterns of transaction, not having obvious economic meaning or legitimate aim

Other circumstances, that suggesting such operations is being carried out for purposes of money laundering and financing of terrorism and financing of proliferation of weapons of mass destruction

Implementation of reissuing the current number with transferring the funds from the legal entity to the natural person

Transfer the funds within a short period of time to the account that differ from the account at which such funds were credited earlier

Profile of suspicious operation



- Analytics of uncharacteristic transactions

- Interaction with Compliance to build a typology of suspicious transactions

- Coordination Rosfinmonitoring (the Federal Financial Monitoring Service) using of new criteria unusual transactions

Tendencies



Refusal from using funds in favor of electronic means of payment



Involvement in dubious schemes socially disadvantaged population groups



Formation of geographic locations

Analytics of uncharacteristic transactions

Interaction with Compliance to build a typology of suspicious transactions

Coordination Rosfinmonitoring (the Federal Financial Monitoring Service) using of new criteria unusual transactions

Compliance



Examination of unusual transactions



Definition of typical indications of operations

Interaction with the whole market participants



Consideration of complete cycle by cashflow



Formation of typology to determine suspicious transactions

Analytics of uncharacteristic transactions

Interaction with Compliance to build a typology of suspicious transactions

Coordination
Rosfinmonitoring (the Federal Financial Monitoring Service)
using of new criteria unusual transactions

Rosfinmonitoring

Private office

Relevant typologies and indicators of dubious operations

New types of risks of doubtful transactions

Sectoral risk assessment

Quality assessment of internal control

Analytics of uncharacteristic transactions

Interaction with Compliance to build a typology of suspicious transactions

Coordination
Rosfinmonitoring (the Federal Financial Monitoring Service) using of new criteria unusual transactions

■ International partnership





Exchange best practices



Regional specificities



Direction of migration



Transboundariness of payment