



THE THIRD ANNUAL EAG CONTEST AMONG FINANCIAL INSTITUTIONS OF THE MEMBER STATES

for the best AML/CFT financial analysis

The EAG Secretariat announced the IIIrd Contest for the best financial analysis in AML/CFT among compliance specialists of financial institutions of the Member States of the Eurasian Group on Combating Money Laundering and Terrorist Financing.

The annual Contest aimed to disseminate of the best practices and lessons learned to improve the effectiveness of national AML/CFT systems and the efficiency of international private sector AML/CFT collaboration. The competition provides a library of best practices that contribute to strengthening the capacity of regional AML/CFT cooperation, as well as a platform for demonstrating practical examples of the identification of ML/TF cases that can be used for training and education of the staff of the national AML/CFT systems of the EAG Member States.

Financial institutions had submitted their best cases of financial analyses selected by the EAG delegations as contest materials in the following areas:

- identification of suspicious customer activity related to drug trafficking, corruption offences, illegal activities in the financial market and illegal gambling activities (including online casinos), budgetary abuse;
- use of technological solutions and new techniques to identify suspicious transactions related to virtual currencies;
- identification of other transactions or customer activities related to money laundering or financing of terrorism.

The final of the IIIrd Contest took place in October 2024 at the “Sirius” federal territory in Sochi on the margins of the IV International Olympiad on Financial Security. The winner and laureates, including the winner of the Audience Award, were awarded in November 2024 at the 41st EAG Plenary.

► Contents

3	Case 1 Financial Analysis Case Study of Ataix Eurasia Ltd Crypto Exchange Compliance Division Mr Aidyn Mukashev, Compliance specialist of the Ataix Eurasia Ltd (crypto-exchange)
---	---

7	Case 2 Bullet points to contest materials for financial analysis case study implemented by OAO Belgazprombank in 2023-2024 Yevgeniy Sizikov, Head of Compliance Control Division OAO Belgazprombank (Minsk)
---	--

11	Case 3 Identification of vulnerabilities in combating terrorist financing when the identity of listed persons is changed Mr Dilshod Ishkuvatov, Head of the AML/CFT/CPF Internal control division of the National bank of Uzbekistan
----	--

20	Case 4 Suspected Terror Financing through ATM withdrawals using multiple foreign cards at sensitive locations Mr Sachin Nambiar, Vice-President of the HDFC Bank, Republic of India
----	---

22	Case 5 Example of the Financial Analysis of Compliance by a "Rysgal" JSCB Division: detection of money laundering through trade transactions Mr Rahymberdi Nuryyev, Head of the Financial monitoring and control over the transactions of the JSCB "Rysgal", Turkmenistan
----	---

25

Case 6

Within the framework of implementation of the policy on organizing internal controls for the purpose of anti-money laundering and combating the financing of terrorism

Mr Nurbek Berdykulov, Head of the Compliance control division of the OJSB "Keremet bank", Kyrgyz Republic

36

Case 7

Attack in the digital world: phishing, carding and cryptocurrency money laundering schemes

Mr Khurram Rizoev, Senior officer of compliance service of CJSB "International bank of Tajikistan", Republic of Tajikistan

40

Case 8

Tax Avoidance Scheme via consumer cooperative terminals installed at dental chain clinics

Mr Aleksandr Popov, Director on financial monitoring and compliance of the PJSB Rosbank, Russian Federation

Case 1

Financial Analysis Case Study of Ataix Eurasia Ltd Crypto Exchange Compliance Division

Mr Aidyn Mukashev, Compliance specialist of the Ataix Eurasia Ltd (crypto-exchange)

A resident individual of the Republic of Kazakhstan made several attempts to replenish his wallet with fiat money by means of card replenishment. A number of attempts had an “error” status and the money did not pass to the client’s exchange wallet. However, several attempts were successful and the money was received in different currencies. After that, the client bought USDT with all the money received by means of the “quick purchase and sale” function (at a fixed rate of purchase and sale) and transferred it to a different crypto wallet.

Cards “error”



- A number of attempts to make card replenishments
- The majority of attempts had an “error” status
- Quick exchange and withdrawal

DECISION No. 1: For the analysis purposes, the company decided to transfer all the transactions to manual confirmation in case of two unsuccessful replenishments and to introduce a warning. The above setting was also implemented in the risk management system at the IT level on a permanent basis and frequent errors and cancellations of transactions were to be treated as “Abnormal wallet activity”.

DECISION No. 2: Meanwhile, a search for similar or duplicated data was carried out.

TRIGGER No. 1: At the same time, there were system notifications on account of “geographic location”, i.e. transactions conducted in geographic zones other than the usual location of the client.

TRIGGER No. 2: As part of the prohibition on replenishment and withdrawal by third parties, notification “if the recipient’s wallet address is different from the previous permissible ones” triggered.

In this way, a number of other resident individuals of the Republic of Kazakhstan were identified who had performed transactions similar to the above scheme. Several individuals whose mail addresses differed in one character only replenished wallets at the crypto exchange with fiat money, made fast exchange and withdrew it to other crypto wallets of other individuals.

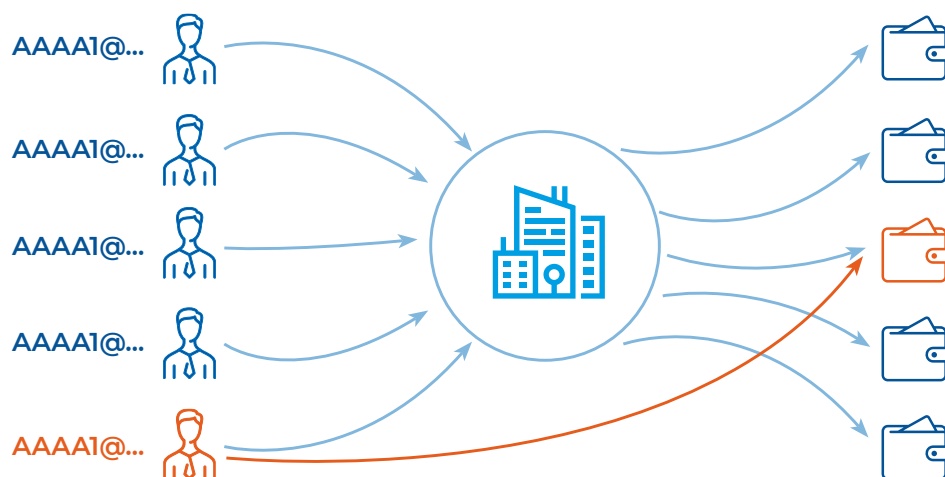
According to the information provided by the acquirer bank, the said citizens of the Republic of Kazakhstan used cards of the Kazakhstan banks, as well as of foreign banks. The system notifications allowed us to find out that all the requests for withdrawal of crypto currency had come from IP addresses located in the Republic of Algeria (*VPN could be used*).

As a result, 2 absolutely identical schemes were identified, i.e. 2 groups worked.

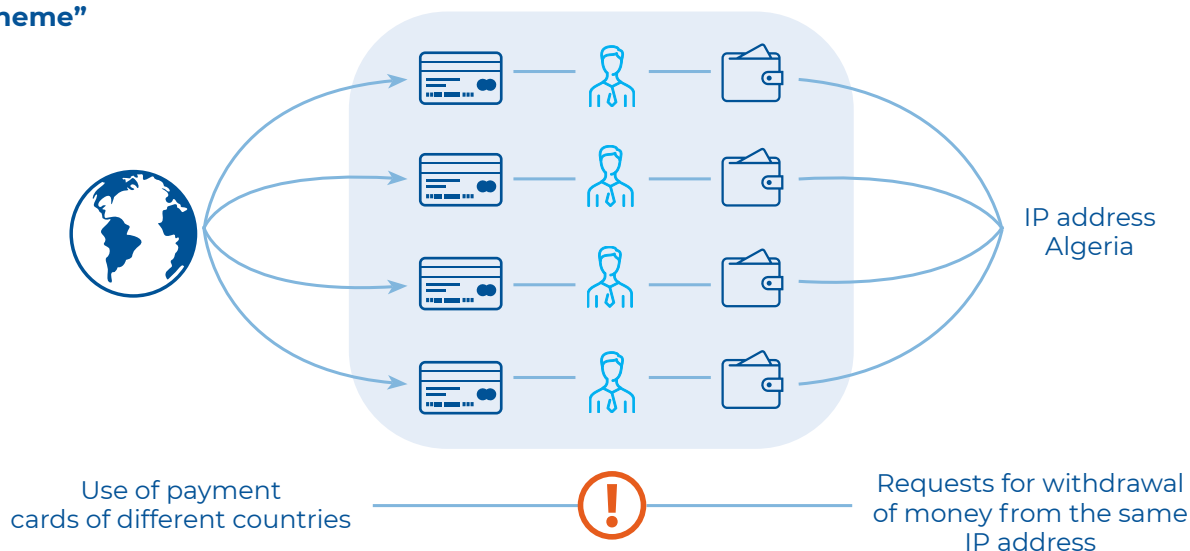


It is important to note that all the clients had a “tutor” since the said clients sent money to their own wallets, as well as to his wallet.

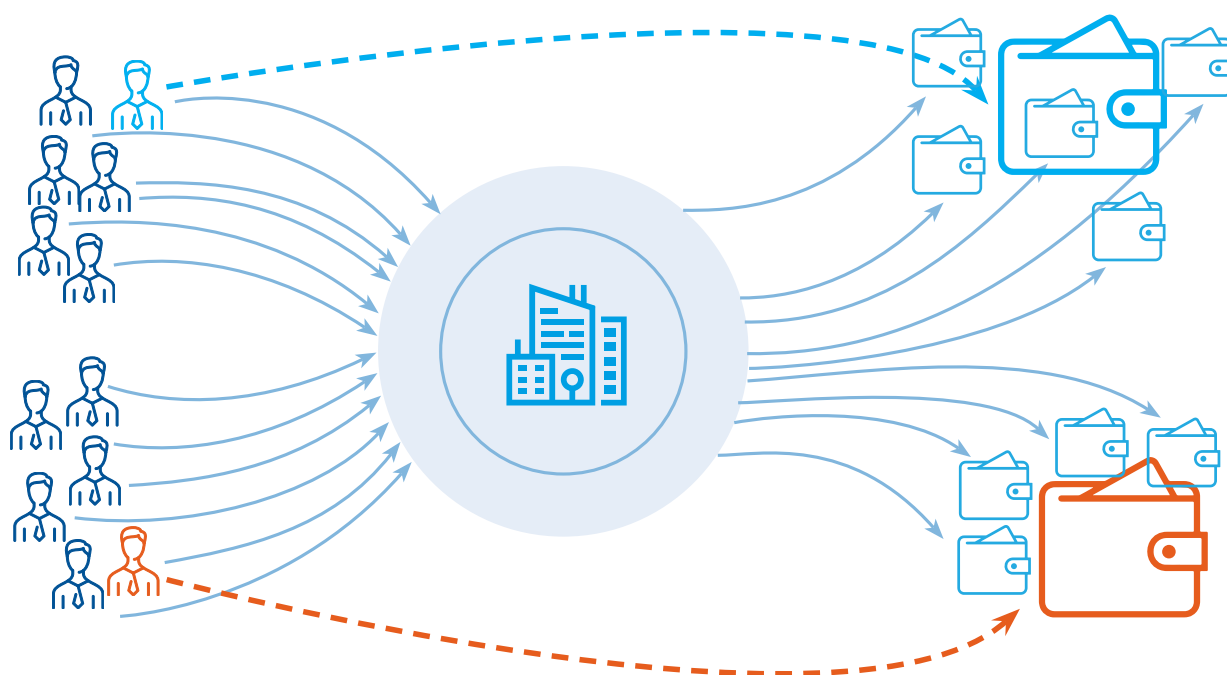
“Group”



“Scheme”



“Scheme X2”

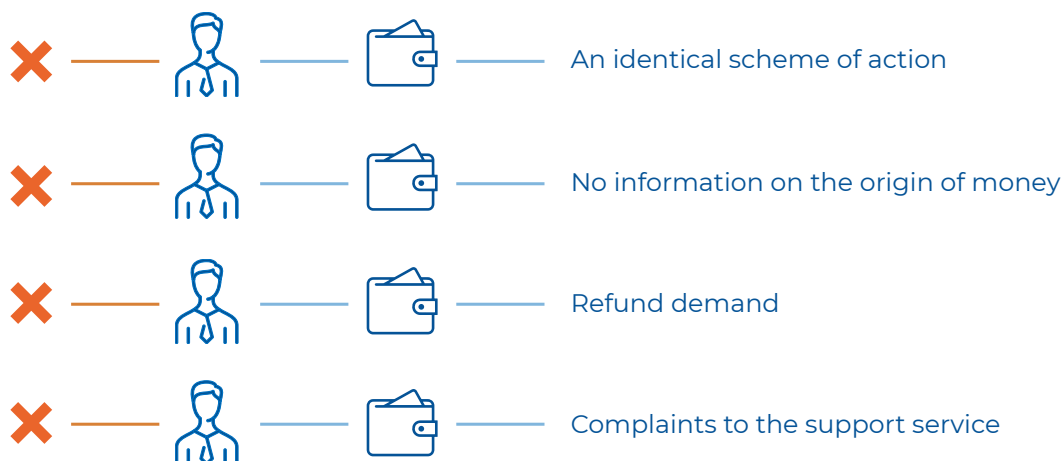


Considering that:

- Identical schemes of action were identified,
- Confirmations of the origin of money were requested from clients, no replies were received.
- The company's support service received letters demanding refunds in Russian with obvious grammatical and morphological errors, which indicates that the account could be used by a different foreign person (*the account was sold or a citizen of the Republic of Kazakhstan passed through the identification for a fee*).
- In addition, a foreign individual reported that money had been debited from his card account. But he denies performance of the transaction.

Accounts of the clients were blocked, wallets were frozen and transactions were suspended.

Blocking



Proceeding that:

- ✓ The said citizens of the Republic of Kazakhstan made replenishments or attempted to make replenishments from card accounts of foreign states (transactions were suspicious in that we see in the system many unsuccessful attempts of replenishment over a short period of time and 1–2 successful ones, meaning that the user failed to perform 3D Secure, i.e. to enter the correct code from a text message);
- ✓ Use of the “quick purchase and sale” function is not always expedient;
- ✓ With regard to all of the above clients, requests for withdrawal of crypto currency originate from IP addresses in Algeria;
- ✓ Mailing names of all clients are unusual for our region (hotmail, yahoo, etc.) + names of certain accounts are Arabic and accounts are verified by citizens of the Republic of Kazakhstan having Slavic full names;
- ✓ All the clients have similar e-mail addresses which differ in digits in ascending order. (example: aaaal@..., aaaa2@..., aaaa3@..., etc.;
- ✓ Several clients made attempts to withdraw money to 1 wallet.

Considered that the money had been raised through fraud or phishing attack and intentionally transferred to other crypto wallets over a short period of time and reported the aforesaid transactions to the RK FIU (11 reports on suspicious and suspended transactions). June – July 2024.



At the beginning of September 2024, internal affairs authorities demanded transaction data from the Company. In this way, we became aware that a criminal case under “Fraud” article had been instituted in a city of the Republic of Kazakhstan and details of the criminal case completely coincided with the details of the aforesaid scheme. The hypothesis has been confirmed and as of today, the law enforcement authorities have grounds for further criminal prosecution.

Case 2

Bullet points to contest materials for financial analysis case study implemented by OAO Belgazprombank in 2023–2024

**Yevgeniy Sizikov, Head of Compliance Control Division
OAO Belgazprombank (Minsk)**

A ML scheme detected by OAO Belgazprombank in 2023–2024 and finally implemented in 2024 through termination of servicing the ML scheme participants and institution of 5 criminal proceedings is presented for taking part in the contest.

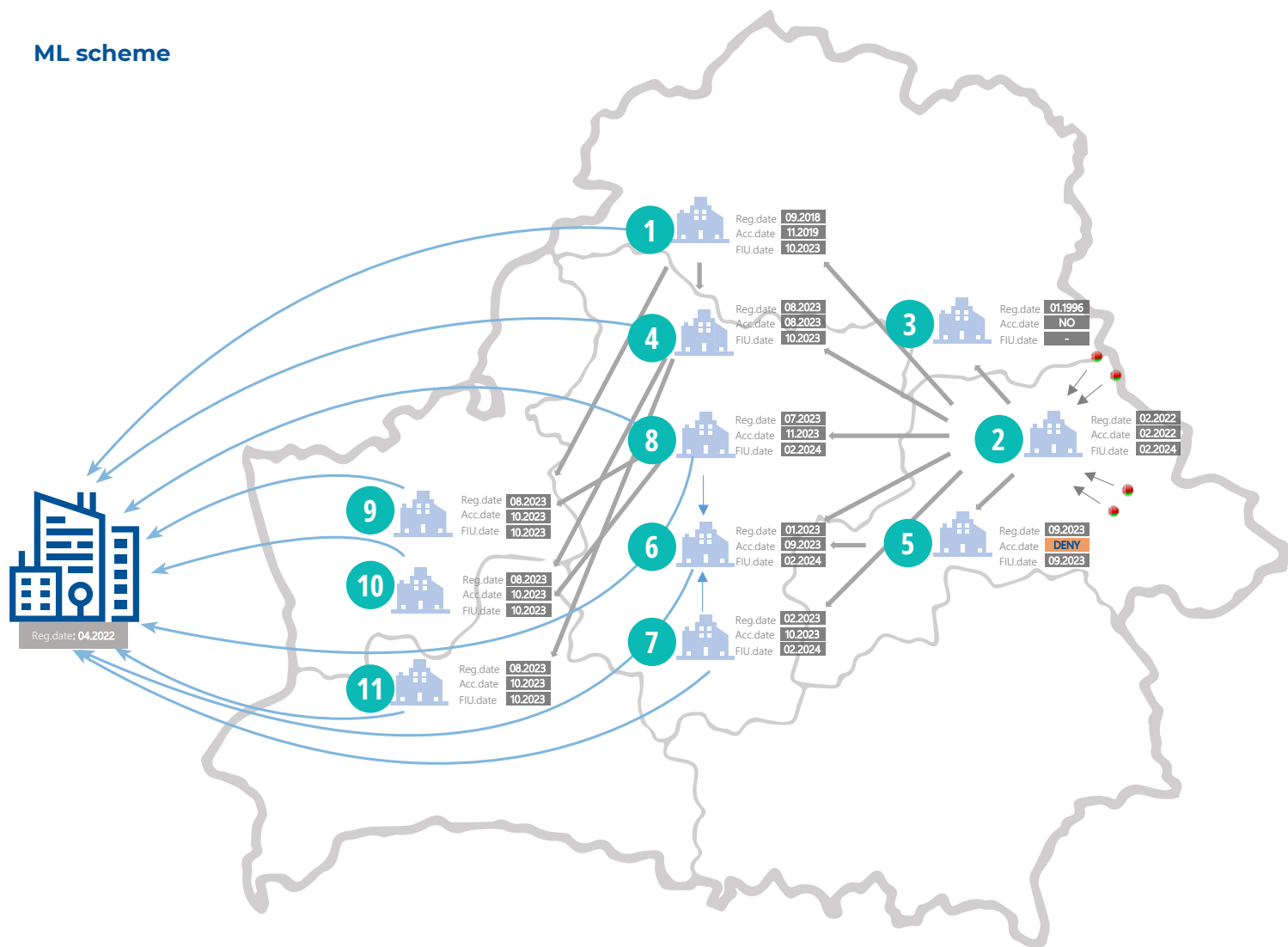
The ML scheme participants: numerous legal entities (the Republic of Belarus) and a foreign legal entity.

Participants of the case implementation



The ML scheme lies down to inflow of money from other banks of the Republic of Belarus from several payers (the Republic of Belarus) to an account of one legal entity (the Republic of Belarus) with subsequent distribution of this money in several steps among many other legal entities (the Republic of Belarus) and siphoning this money off in favor of a foreign legal entity (the European Union) through several bank transfers.

ML scheme



The ML scheme stages

- ✓ A number of new legal entities was registered in 2023 (the Republic of Belarus);
- ✓ Most of them opened accounts with the Bank;
- ✓ Opening of an account with the Bank was denied to one of the legal entities;
- ✓ The founders and/or directors changed at several previously established legal entities (the Republic of Belarus) who had earlier opened accounts with the Bank;
- ✓ Financial transactions were started in October 2023 with subsequent siphoning the money off in favor of a foreign legal entity (test transactions were conducted as part of the declared activities for relevant amounts, which reduced (prevented) the opportunity of detecting (including automated detection) them at the initial stage;



A manager of one of the clients (business unit) noticed that the questions of the director of one of the legal entities about the possibility and “security” of financial transactions for cash withdrawal using a corporate bank payment card were suspicious and informed the executive officer (hereinafter the EO) of the Compliance Control Division to that end;



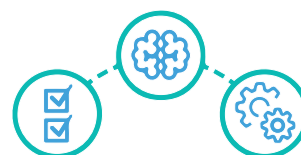
Work of the EO with this ML scheme: the EO sent questions to the director of the legal entity, identified the money flow that involved transactions with siphoning off abroad, identified a chain of similar transactions and their participants, performed work with regard to other identified legal entities;



Reports were provided to the Financial Intelligence Unit in two stages, servicing through a remote banking system was suspended. In addition, a representative of the Financial Intelligence Unit was contacted in order to make a point of this information;



Activities on accounts of all companies were terminated (transactions were arrested or suspended by virtue of resolutions of competent authorities) and/or accounts were closed).



Special features of the ML scheme (success criteria):

1. **High level of competence of the officers**, dealing with clients (noticed the clients' interest in suspicious financial transactions, noticed behavior pattern of a representative of the legal entity at the time of accounts opening);
2. **High level of competence of the EOs** (elaborated and understood the ML scheme beyond the initial suspicious transactions; identified and elaborated resumption of the ML after the recess);
3. **High level of interaction between:**
 - Business units and the Compliance Control Division;
 - The Bank and the Financial Intelligence Unit;
 - The banking system and the banking regulator.

Special features of the ML scheme (possible connections and obstacles):

Possible connection:

- close dates of registration of new legal entities;
- close dates of change of founders and/or directors of the previously established legal entities;
- minimal amount of the authorized capital;
- minimal number of employees (normally 1);
- individual legal entities are located at one address or at closely adjacent addresses;
- no websites or information on the Internet;
- difference between the phone numbers at the website of the register of legal entities and those submitted to the Bank;
- registration of e-mail addresses mainly with the same mailing service and using similar approaches to generation of the user name in the e-mail address structure (no personal e-mail addresses, use of names of legal entities, etc.);
- individual financial transactions are performed by different legal entities using identical unique numerical identifiers of devices in the computer network (IP addresses);
- identical activities of legal entities (construction operations, postal and courier activities);
- no tax payments in support of business activities;

- quality of documents (suspicion about their reliability (especially cargo shipping ones), as well as suspicion that individual documents of different legal entities were made according to identical templates.



Obstacles to detection:

- no overlaps in terms of founders, directors, accountants across all legal entities;
- amounts of financial transactions within the threshold limits;
- identical subject matters of payment purposes as part of the activities (construction and cargo carriage);
- no peculiarities about the age of founders and/or directors (mainly around 35–40 years of age, the youngest—22 years of age (a single case));
- personal appearance and behavior of the majority of representatives did not raise any questions.

The Financial Intelligence Unit assumed,

that financial transactions of a group of entities were aimed at illegal generation of income, including embezzlement of public funds. The criminal scheme involved the use of such tools as organizations having signs of shell companies in their activities.

Special features of the ML scheme (key takeaways):



Short time period

from the transactions start date till termination of transactions and institution of criminal proceedings



Money was seized and account transactions

of 6 legal entities were suspended by virtue of resolutions of public authorities



The bank blocked

4 corporate bank payment cards



Account opening was denied

to 1 legal entity



17 reports

to the Financial Intelligence Unit



Institution of 5 criminal proceedings

The law enforcement authorities established that the bank clients booked knowingly counterfeit primary accounting records of supply of commodities and materials and performance of works (services). These illegal activities resulted in underpayment of taxes equivalent to millions US dollars.

Case 3

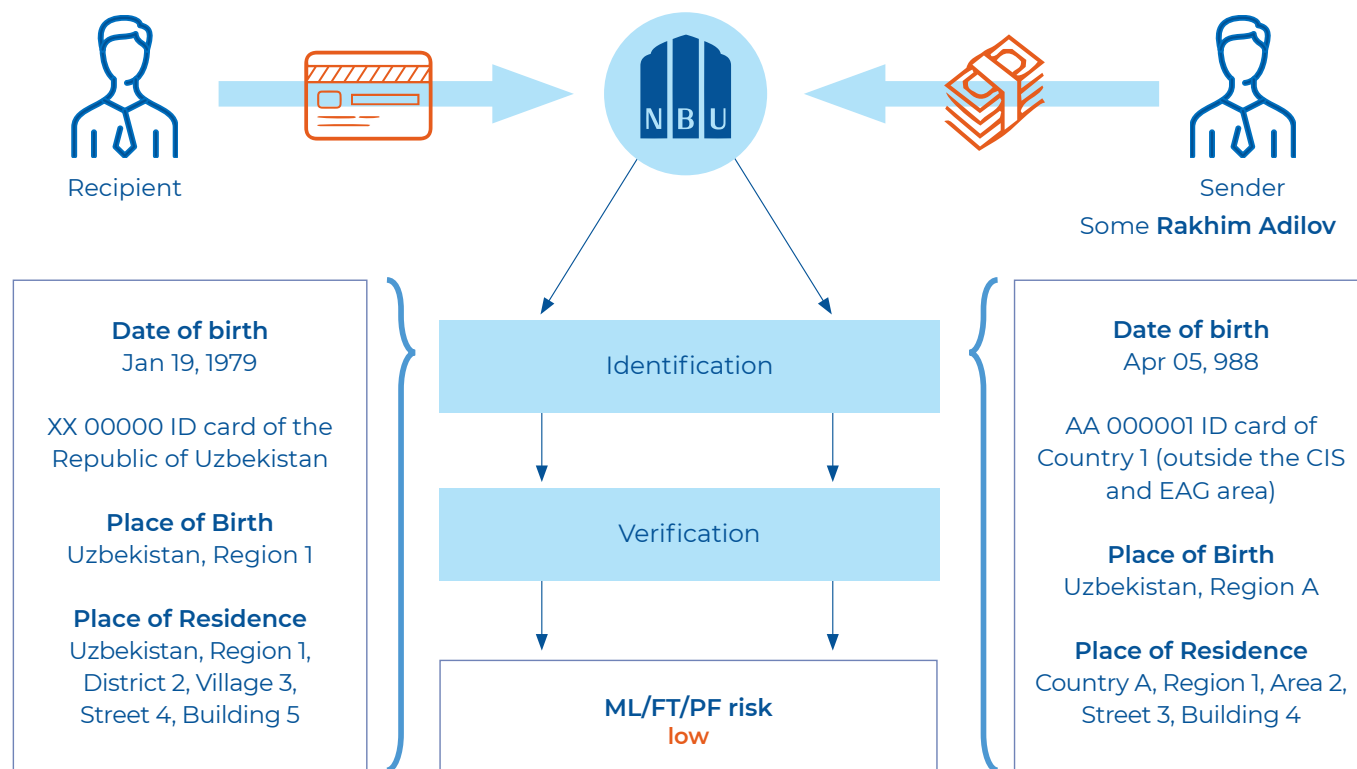
Identification of vulnerabilities in combating terrorist financing when the identity of listed persons is changed

Mr Dilshod Ishkuvatov, Head of the AML/CFT/CPF Internal control division of the National bank of Uzbekistan

This case study has exposed a TF countering vulnerability associated with the revision of identification data in the national CFT system.

An individual, let's call him the Recipient, requested the National Bank's Department for Region A to issue him with USD 400 remitted to his name from a Country A via a money transfer service.

Transaction (receipt of money through TIR systems)

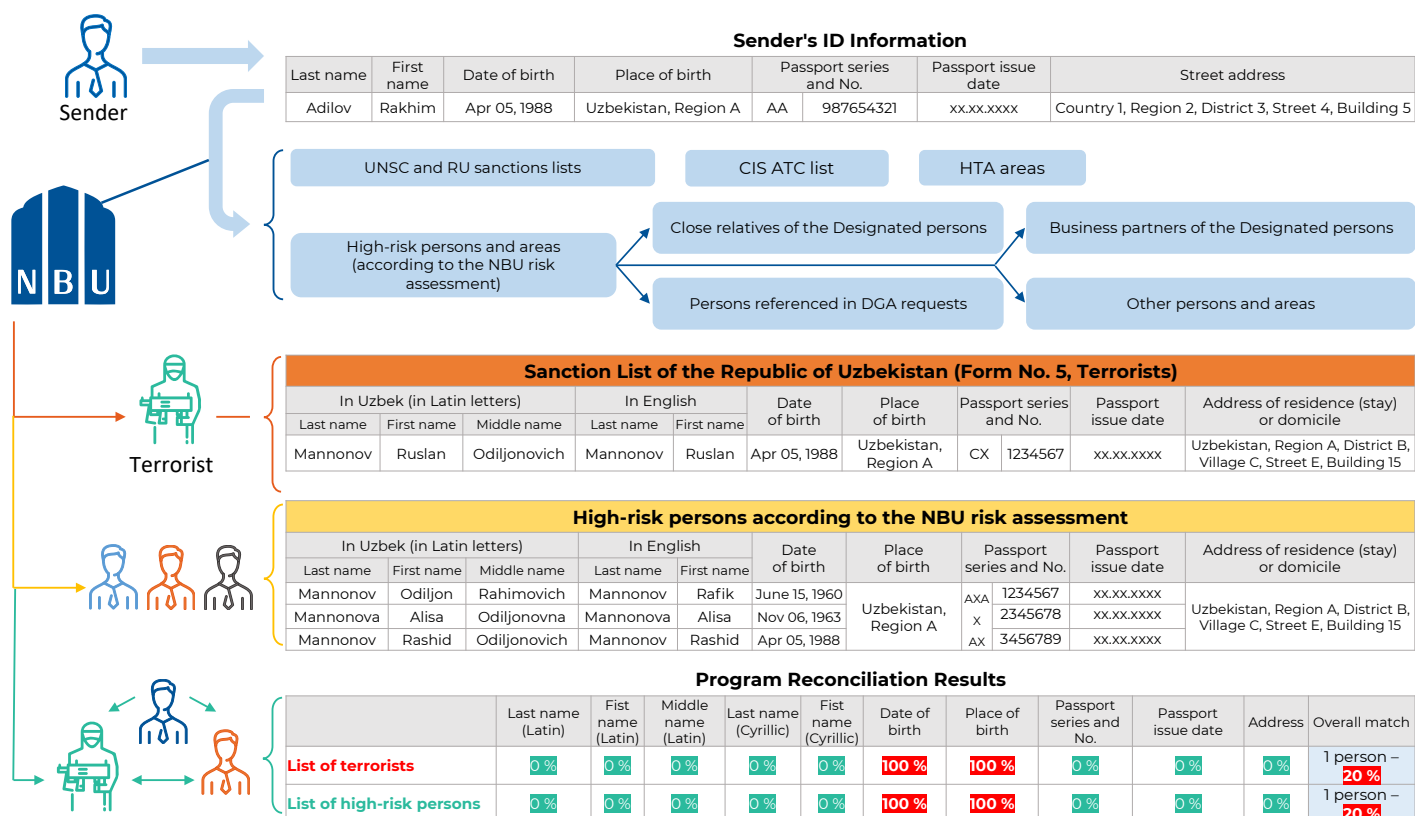


Once the passport was produced, the internal control staff ran the identification check and verified the ML/TF risk of the Receiver whereupon the Receiver's risk was classified as **'minimum'**.

Finally, the bank's internal control officers identified the sender as the individual named Rakhim Adilov (the first and last names are changed). The check rated Rakhim Adilov as being a low risk in terms of ML/PF.

And as a result, a TF risk verification of the sender Rakhim Adilov was initiated. At this point, I would like to point out that a verification of persons under the TF system is carried out automatically using dedicated software.

Verification of the Sender's FT Risk



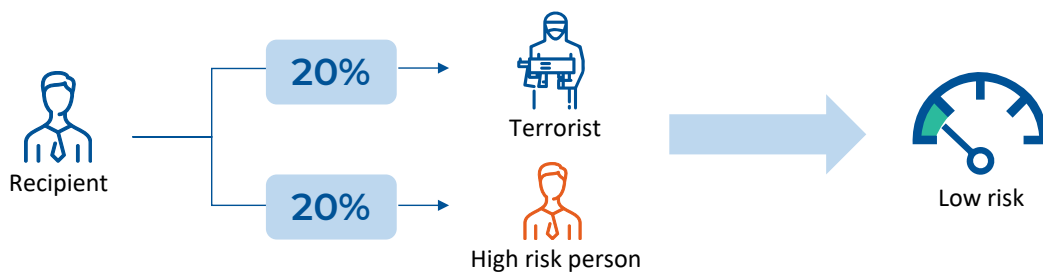
Thus, the program checks out the identification data of Rakhim Adilov as the sender against the identification data of the persons included in the International and National Lists and the persons included in the CIS Anti-Terrorism Center Lists; also, the sender was cross-checked with the persons marked with a high TF risk measured according to the risk assessment performed by the National Bank. I might add that some data on high-risk individuals was submitted to the DGA (dedicated government agency).

Since we had to use assumed first, middle, and last names to present this case study, I would like to express my appreciation to Ruslan Odiljonovich Mannonov, a DGA officer for consenting to use his data as a person on the List.

In this case, dates and places of birth matched and the total degree of matching for these individuals was 20%.

The program identified two separate individuals – one on the National Terrorist Watch List and the other on the High Risk List of individuals – with the sender identification match.

Basis for Conducting a CDD



The bank's staff revealed that



It was decided to

Conduct a CDD

Block 400 \$ for 3 days

If the software check results alone are to be placed in context, the 20% match signals a low TF risk, but the bank staff found that the street address of the recipient and the street address of the person who had had a 20% match with the sender, namely, Rakhim Adilov, were next door to each other.

Subsequent to that, a decision was made to carry out a due diligence of the customer's business partner and block the remitted amount of USD 400 for 3 days.

The CDD found that:

The recipient lived next door to the Designated person having the 20% match with the sender Adilov Rakhim

The recipient lived next door to the father of the Designated person having the 20% match with the sender Adilov Rakhim

The recipient lived next door to the brother of the Designated person having the 20% match with the sender Adilov Rakhim

The sender's last name 'Adilov' had the same root 'Odil' with the name 'Odiljon' and the sender's first name 'Rakhim' had the same root 'Rakhim' with the middle name of the father of the Designated person having the 20% match, so they were likely to be father and son

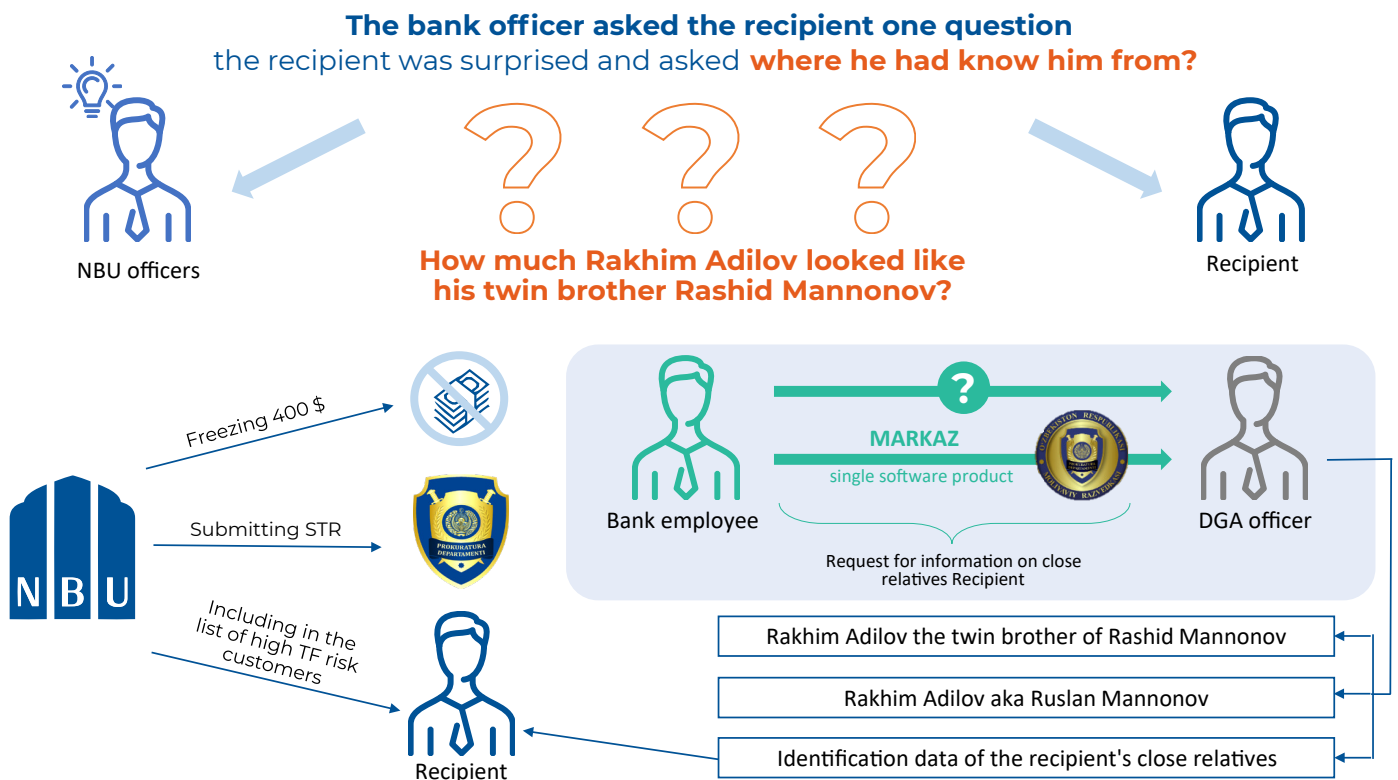
The sender had the same date and place of birth to those of the brother of the Designated person with the 20% match to the sender Rakhim Adilov and, therefore, they were likely to be twin brothers

CDD Results

In accordance with this requirement, the NBU Internal Control Service carried out a financial analysis of the recipient and his close relations turning up the following findings:

- the individual A was a customer at the NBU for several years as he drew his salary from the NBU card being employed as a watchman in a rural kindergarten;
- during 3 years, from the 1st to the 4th day of each month, he received money of the same amount from the son of the individual B from the country B whereupon it was inferred that his son of the individual had been employed in the country A.
- But 7 months following the last receipt of the money, the individual A started remitting different amounts to the name of the individual B's son in the country A with the first addresses of the money transfer being the same as that of the terrorist; some time later, the money was rerouted to the different addresses in the country B bordering the HTA (heightened terrorist activities) stricken area.

Verification of CDD Conclusions



And it was at that point that we found ourselves wondering.

Why the son of the individual A, the individual B, who had been remitting money for 3 years, all of a sudden, started to receive money from his father in the country A 7 months later?

Where did the elderly common rural kindergarten watchman, the individual A, get the money from?

In order to figure out this situation, we started to turn up different documents and during the last risk assessment of the NBU, an out of the way trend of withdrawing cash from one ATM in this region was

spotted. We got to the bottom of the odd trend, and it turned out that several cards had been cashed out at that ATM.

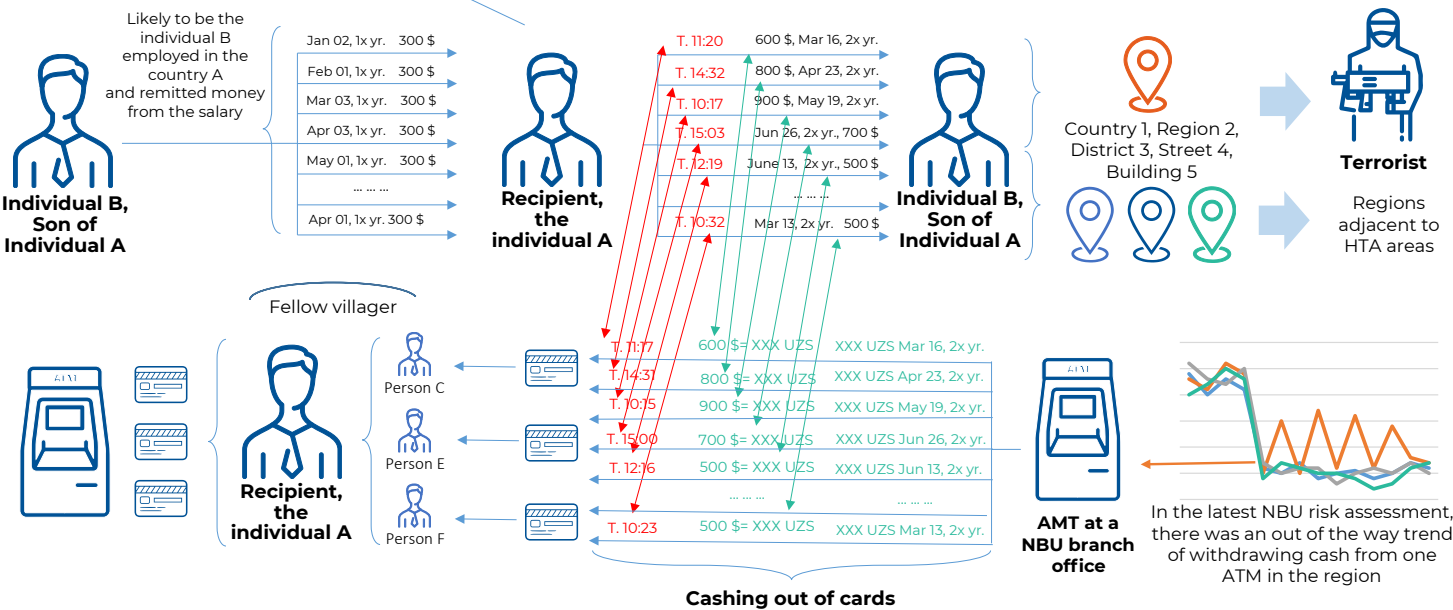
And here's where it gets interesting, the cash-out time and the US dollar equivalent amount matched the time and remitted sums.

Apart from that, the holders of these cards were fellow villagers of the individual A, and the photo captured the individual A in the act of withdrawing cash; also, the branch office staff recognized him, and said that he would first approach the ATM and cash out, and then set out to the teller to remit the money.

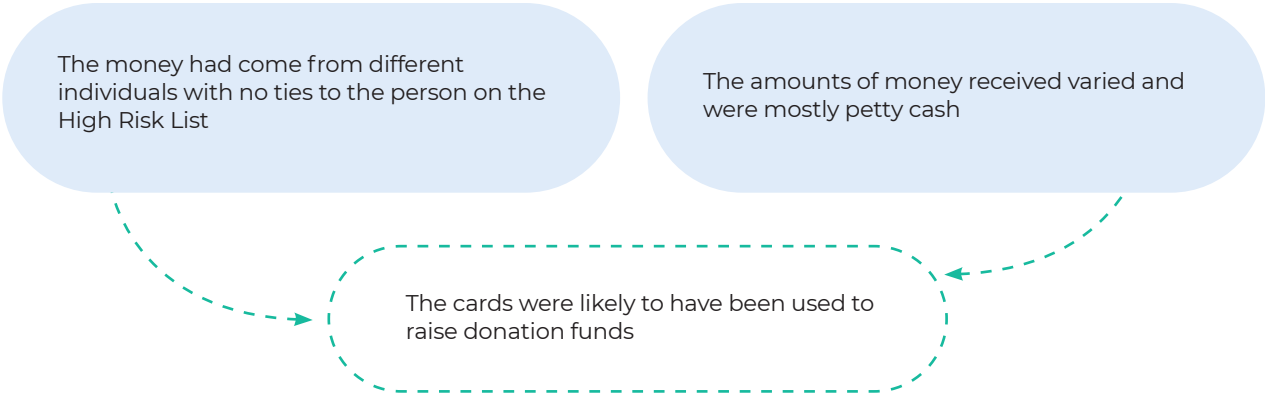
Financial Analysis Findings for the Recipient and His Close Relatives



Payment card of the individual A who drew salaries for being employed as a watchman at the village kindergarten; the expenses are shown only for purchased groceries



The card turnover analysis showed that:



At the same time, another international Visa card shared the same number to which the card under review was linked and the places where it had been used were located in the neighborhood of the street addresses of the individual B.

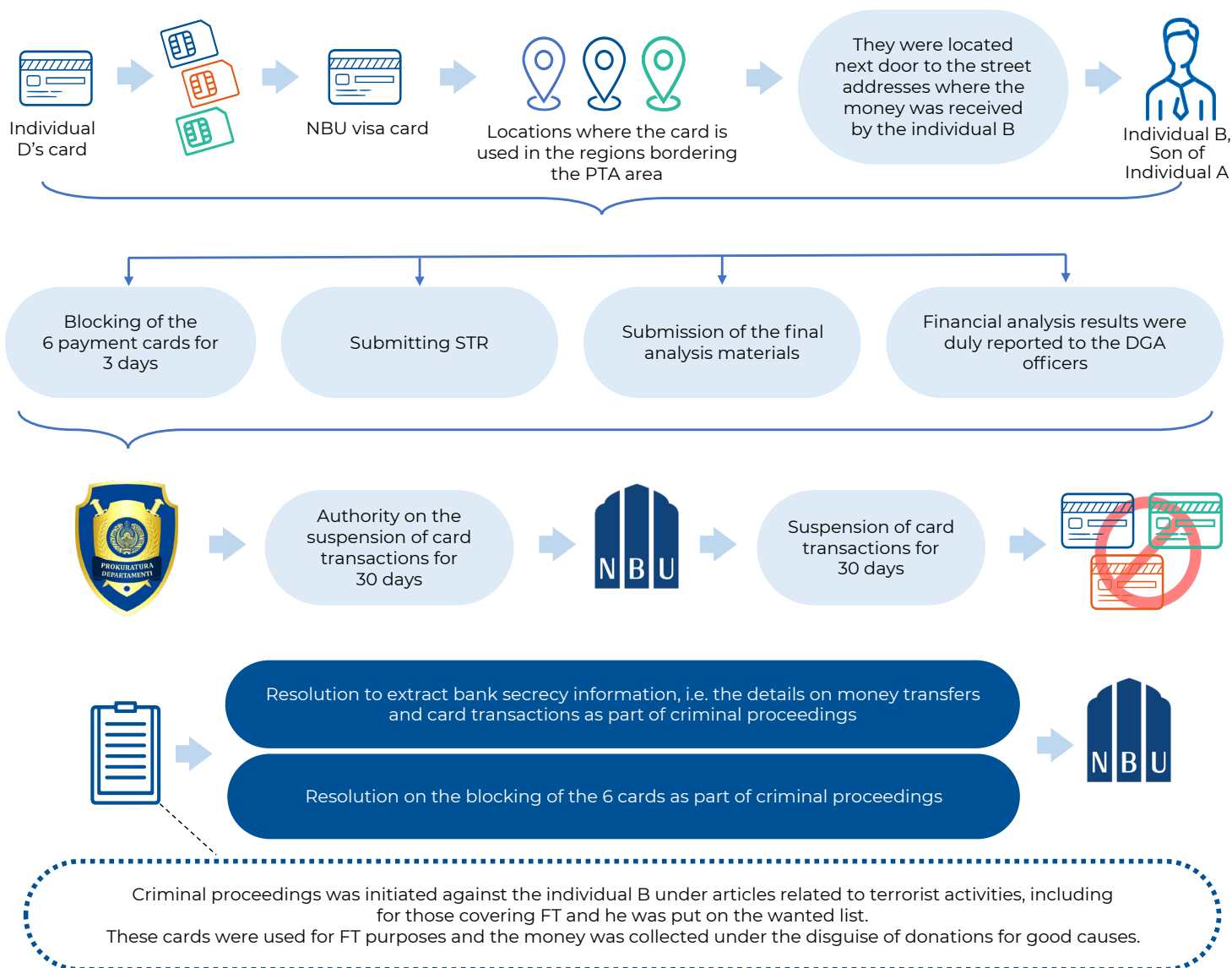
Based on these observations, a conclusion was reached that the identified 6 cards may have been used to collect funds for TF purposes and it was decided to block the 6 cards for 3 days and to send STR and the DGA officer was duly informed of the financial analysis findings and provided with the financial analysis materials.

Two days later, we received a request from the DGA to block the 6 cards for 30 days.

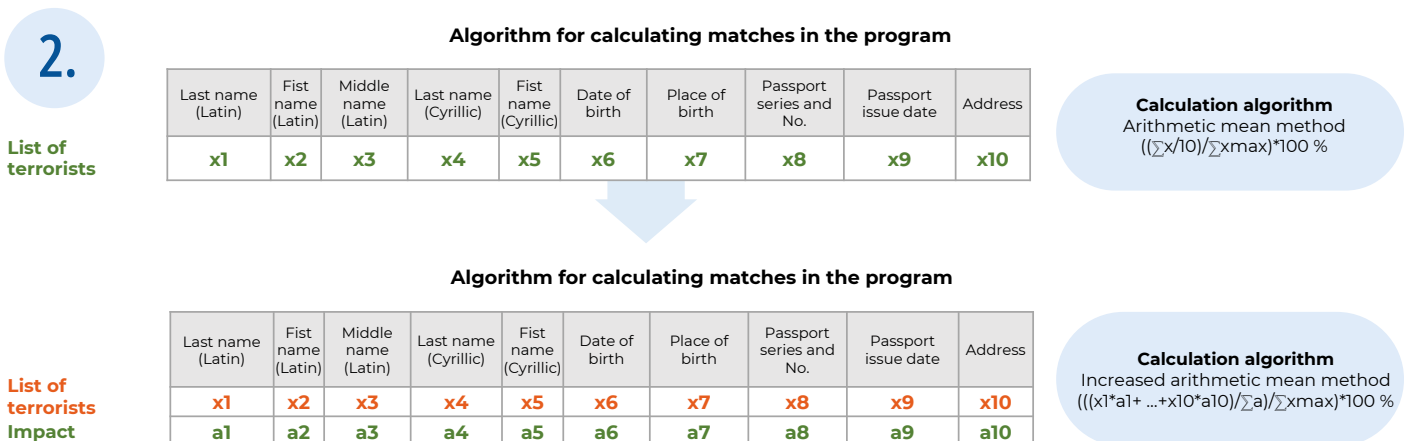
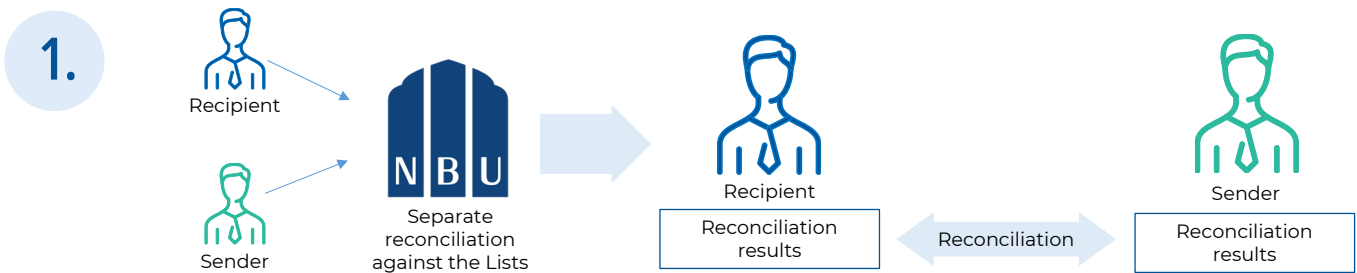
20-25 days later, we received a resolution to extract the bank secrecy information, i.e. the details on money transfers and transactions of the 6 cards as part of criminal proceedings and the Resolution to block the 6 cards s part of criminal proceedings.

This resolution stated that criminal proceedings had been initiated against the individual B under articles related to terrorist activities, including for those covering TF and he was put on the wanted list.

These cards were used for TF purposes and the money was collected under the disguise of a donation for good causes.



Vulnerability Identification and Elimination



Based on this case study, we have identified the vulnerability and taken remedial actions.

First, previously, the software provided a separate reconciliation of the identification data of the parties involved in the transaction, later we added a function to reconcile the verification results of the parties involved in the transaction, i.e. the coincidence check of the identification data of the sender and the recipient.

Second, the algorithm for calculating the match percentage was applied using the arithmetic mean method, but after this case, the algorithm has been changed and currently the arithmetic mean weighted value is being used, i.e. different coefficients were assigned to the identification data based on the likelihood of these data being changed.

Dear colleagues, here in Uzbekistan, the DGA and the supervisory authority on a regular basis conduct training workshops for internal control officers at reporting entities. And in one of these workshops, a DGA officer made a special note of our work on this case study.

According to the information of the DGA officer, using our case, the DGA is pursuing the effort to:

- identify other facts of any changes in the identification data of the persons included in the List;
- identify the evidence of conducting transactions of the persons currently included in the list with updated identification data.



This vulnerability and recommended measures to identify and minimize it are included in the training programs for internal control officers at reporting entities.

Furthermore, putting our case study into perspective, a letter was sent to the supervisory authority providing the basis for:

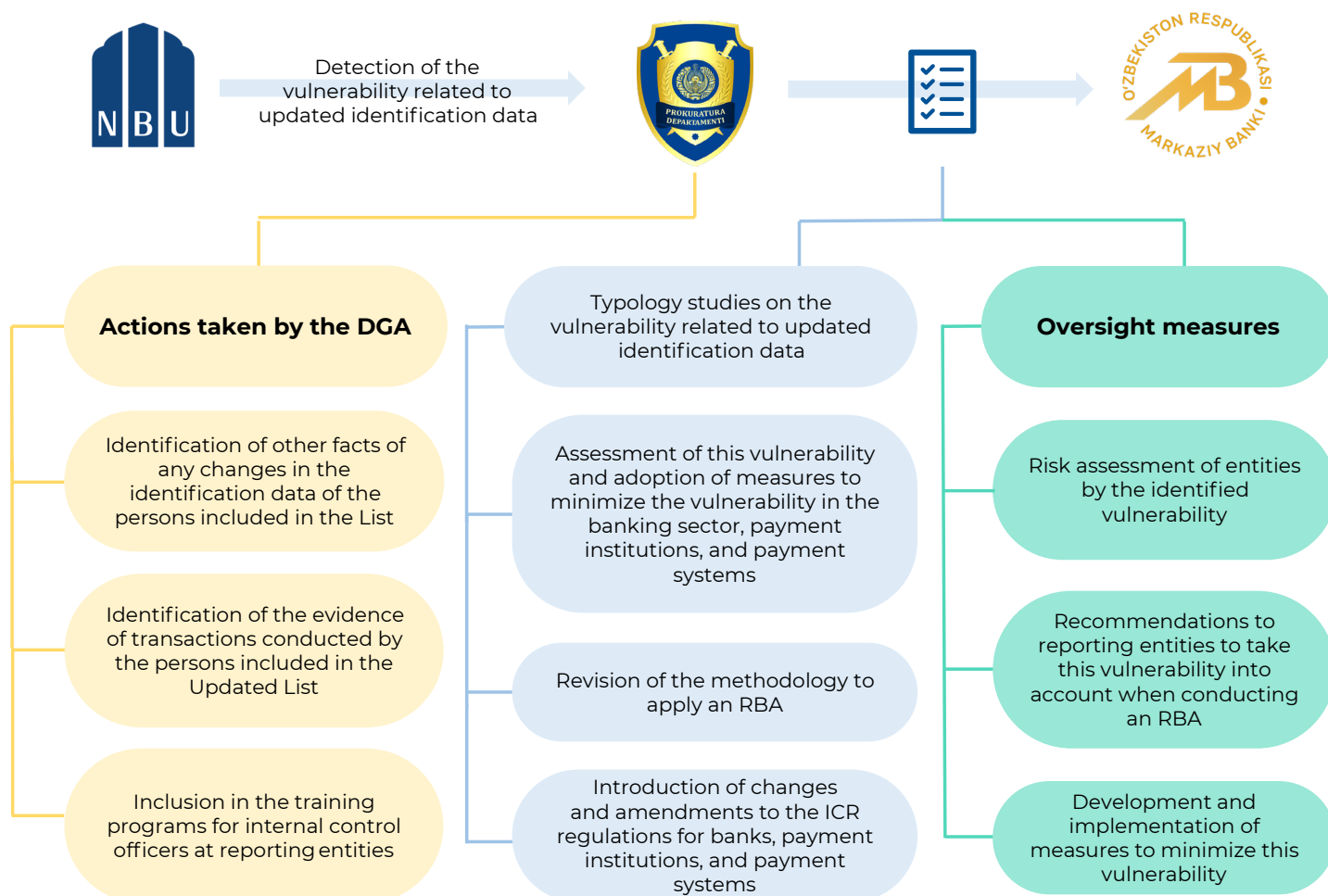
1. A typology study on the CFT vulnerabilities arising from relevant changes in identification data is being conducted providing the basis for:

- this vulnerability will be assessed and measures will be developed and applied to minimize this vulnerability in the sectors of banks, payment institutions, and payment systems;
- the methodology for applying the risk-based approach (RBA) is being reviewed;
- any changes to be introduced if and where needed to the ICR for banks, payment institutions, and payment systems are being reviewed.

2. Appropriate action is being taken oversee this vulnerability leading to:

- the study of the assessed risk exposure of reporting entities in the context of the identified vulnerability and recommended measures to assess this vulnerability are being worked out;
- recommendations were circulated to the reporting entities to take this vulnerability into account when applying a RBA;
- measures are being developed and taken to minimize this vulnerability.

Practical Relevance and Use of this Case Study in the National AML/CFT/CPF System



Case 4

Suspected Terror Financing through ATM withdrawals using multiple foreign cards at sensitive locations

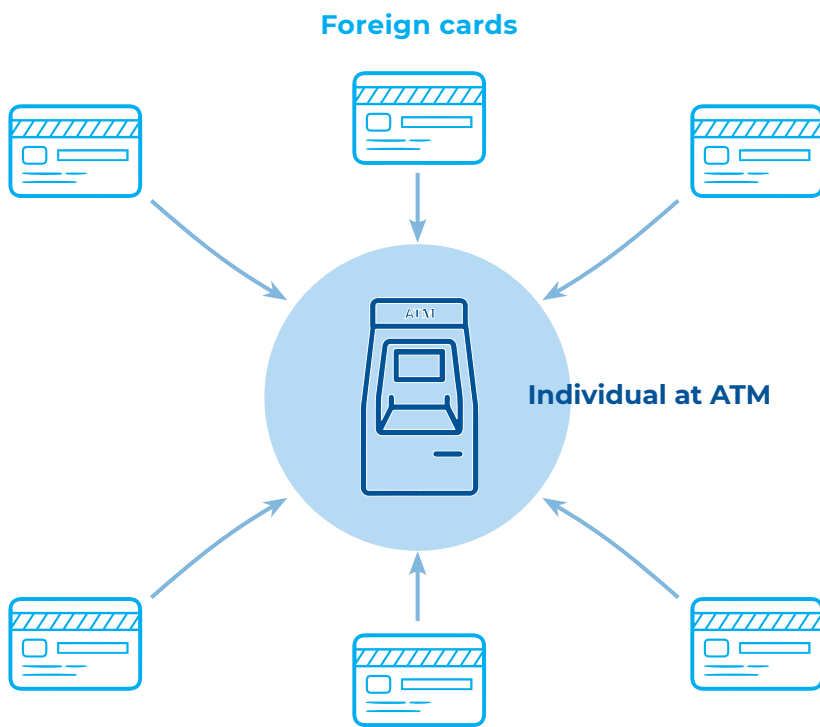
Mr Sachin Nambiar, Vice-President of the HDFC Bank, Republic of India

During an ad-hoc review of ATM withdrawals using foreign cards, a red flag was identified and suspicion raised with concurrent cash withdrawals from a single ATM at a sensitive location. The Data analysis revealed that multiple foreign cards were used concurrently to withdraw cash from one ATM within a span of few minutes. The ATM is located in a sensitive border area prone to high-risk terrorist activities.

Since the said area is not a tourist destination, it does not attract foreigners. Due to the risk of terrorist activities, generally local residents avoid free movement and especially carrying out financial transactions at late night hours. Review of surveillance recording of CCTV camera installed in the ATM indicated that one individual was in possession of multiple cards and used them concurrently. The appearance of the individual did not look like a person from the card issuing country.







To understand the seriousness of the red flag and suspicion observed, media search was performed specifically for the same geographical location, revealed that a terrorist incident had occurred in the same locality just on the previous days of cash withdrawal.



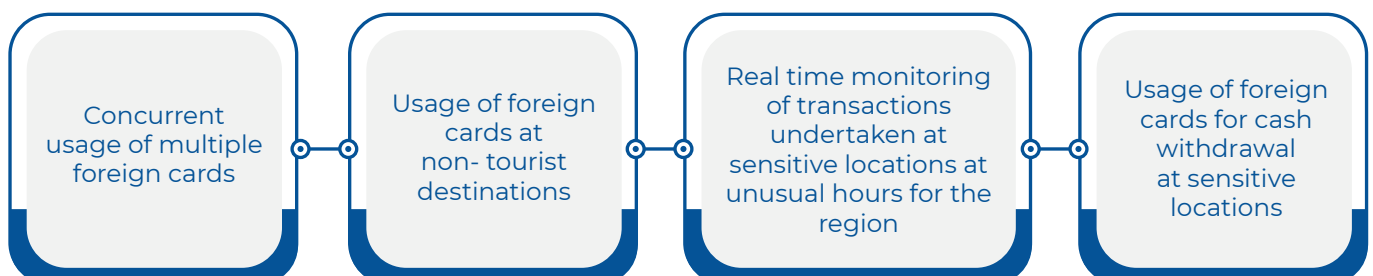


Ad-hoc review in subsequent months for the same pattern performed whereby two more such instances at different sensitive locations in other parts of the country were observed / identified.

Modality and Red Flags

-  An individual was in possession of multiple foreign cards and using them at an ATM concurrently.
-  Six foreign cards were used concurrently withdrawing maximum amount permissible (upper cap fixed by the bank) for acquiring transactions.
-  Since the ATM used is situated at an area prone to high terrorist activities, financial activity at late night hours observed as very unusual, specially by foreign national.
-  Bank Identification Number (BIN) of the foreign cards revealed issuance of cards from a neighboring country.
-  Individual in possession of foreign cards did not appear to be resident of the card issuing country.
-  Incident of cash withdrawal immediately on the next day of terrorist incident raises suspicion of terrorist funding.

Indicators for implementation



Example of the Financial Analysis of Compliance by a "Rysgal" JSCB Division: detection of money laundering through trade transactions

Mr Rahymberdi Nuryyev, Head of the Financial monitoring and control over the transactions of the JSCB "Rysgal", Turkmenistan

Trade transactions (commerce) are (is) inherently complex and intricate reflecting the nature of interconnected supply chains around the globe. Trade naturally serves as a vehicle for both neophytes and 'sharks' in the money laundering industry, as well as for organized criminal groups and terrorist financing networks to grease the wheels for financial flows of numerous activities, including laundering illegal proceeds, such as drug trafficking and terrorist financing which is currently relevant for sanction evasion.



Bank Profile:

- 'Rysgal' Joint Stock Commercial Bank is a wholly privately owned commercial bank that was established in 2011;
- it is a major government bank and one of the three largest banks in the country in terms of active operations;
- the number of customers exceeds 279,000, including local companies and self-employed persons;
- its activities are focused on financing small and medium-sized businesses and large national projects;
- it provides comprehensive settlement and lending services to the commodity flows of exclusively domestic privately owned businesses with their business partners in foreign countries;
- it plays an active role in government programs for the development of the nation's private sector.



Trade (trade transactions) will retain an incentive for organized criminal groups, professional money launderers, and terrorist financiers/organizations that will illicitly exploit this sector, a product or a service whenever an opportunity presents itself.

In this context, the main goal of compliance officers is to be vigilant to global supply chain players.

The bank identified a suspicious customer named 'G' who recently was an individual entrepreneur (self-employed person), specifically between 2021 and 2022. The individual entrepreneur, i.e. customer 'G' at the bank set in motion funds on bank accounts to foreign companies, including cash of a certain amount in the national currency being deposited in his current account for the purpose of subsequent conversion and transfer to the accounts of his business partners represented by foreign companies 'Zh' and 'Sh' registered

respectively in countries 'T' and 'D' at that time being the countries with a system falling short of the FATF standards.

- ✓ Compliance officers promptly implemented expanded control measures and initiated a preliminary analysis of the banking operations of the Bank's customer 'G'.
- ✓ The existing telltale signs set the scene for an initial analysis to be kick-started by compliance specialists. That is, the bank's available information was garnered through the use of its own database and publicly available information on the web.
- ✓ The Bank's staff requested from the Bank's client 'G' additional documents and information on relations with counterparties of the foreign companies 'Zh' and 'Sh'.
- ✓ The Bank's customer 'D' could not give a proper account for the situation citing as the reason that he was out of the country at the moment.
- ✓ Thus giving rise to suspicions of close relationships being maintained between the Bank's customer 'G' with the business partners at the foreign companies 'G' and 'S'.



These measures were implemented in order to ascertain the target use of converted funds by the Bank's customer 'G' for payment to the foreign companies 'Zh' and 'Sh' under a food product import contract.

The preliminary analysis of all counterparties that had had commercial dealings with the bank's client 'G' revealed several foreign companies, such as companies 'G' and 'S' registered in the countries 'T' and 'D' respectively, the beneficiary of which was the businessman, the bank's customer 'G'.

These foreign companies 'Zh' and 'Sh' registered in the countries 'T' and 'D' were also used as intermediaries in entering into contracts with other residents of Turkmenistan to encourage price speculations for goods imported into the country, to conceal the true income, the failure to pay taxes in accordance with the tax legislation, and the withdrawal of capital.



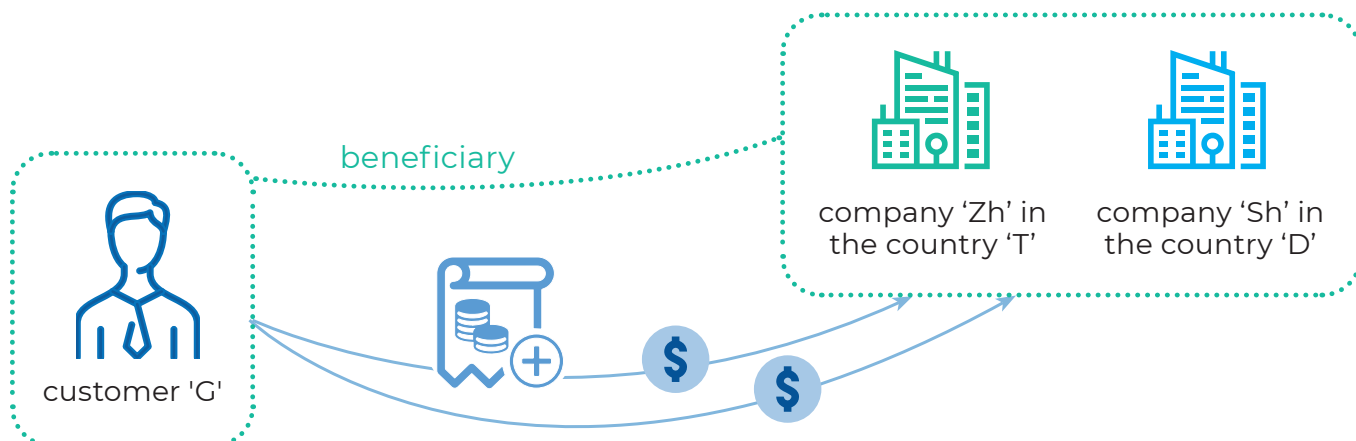
The initial analysis uncovered the evidence of suspicious business comings and goings and underlying suspicious transactions. The bank duly and timely filed several suspicious transaction reports on bank's customer 'G' with Turkmenistan's Financial Monitoring Service.



In the light of the information shared between the bank, Turkmenistan's financial intelligence unit and other relevant authorities it transpired that during the time period in question, the Bank's customer 'G' had been the beneficiary of its business partners, i.e. the foreign companies 'Zh' and 'Sh' registered in the country 'T' and 'D' contracted to import food product and had transferred certain amounts in foreign currency from his bank account in several transactions over a certain period of time.

The STR was generated on suspicions that the transactions had resulted from the collusion between the importer and the exporter.

It was found that the bank's customer 'G' entered into contracts with and transferred funds to the accounts of the partnered foreign companies 'Zh' and 'Sh' where he himself was the beneficiary for food product imports.



This businessman, the bank's customer 'G', attempted to apply a common method of money laundering in trade transactions by overstating invoiced amounts for goods and services. The key element of this method is known to be the falsified price for goods or services in order to misrepresent the value equivalent. In a scheme of this type, the critical aspect is the complicity of the importer and exporter in the misrepresentation.

Furthermore, according to the relevant customs reports, it was revealed that the prices of imported food products had differed by a wide margin from those quoted upon shipment of goods from the country of origin (the so-called gray imports).

According to the legal requirements, Turkmenistan's financial intelligence unit conducted an objective analysis on STR received from our bank as a reporting financial institution.

As it soon became known as a feedback from Turkmenistan's FIU, based on the findings of the prompt analysis of the information by the FIU and the relevant materials provided by the bank, appropriate arrangements were made to submit the materials of the joint financial investigation to a competent agency, that in turn undertook a comprehensive inspection and investigation leading to the person involved in this case being prosecuted under the Turkmen law.



By spotting the issue and properly compiling information on the suspicious transaction of the bank's customer 'G', our financial institution as an entity reporting under the AML/CFT/CPF framework made its input in support of the operational needs of Turkmenistan's Financial Monitoring Service.

Case 6

Within the framework of implementation of the policy on organizing internal controls for the purpose of anti-money laundering and combating the financing of terrorism

Mr Nurbek Berdykulov, Head of the Compliance control division of the OJSB "Keremet bank", Kyrgyz Republic

Customers' suspicious actions were identified as part of the compliance control process, and their accounts were closed. The main factors contributing to this decision were the following:

1. Unreasonable account activity: A disproportionately high frequency of transactions compared to previous months raised the bank's concerns.
2. Abnormal transaction amounts: Large transfers that lack clear economic justification or are inconsistent with the customer's financial situation.
3. Strange geographic destinations: Receiving and sending funds to jurisdictions with a high risk of money laundering or terrorist financing.
4. Lack of transparency: Customers failed to provide the necessary documentation to confirm the source of funds, posing additional risks.
5. Forgery of signatures in contracts: Forgery of signatures in contracts is a serious offense that can result in criminal charges. This act is typically classified as fraud or forgery of documents. Most countries impose stiff penalties, such as fines and prison sentences.

Analysis of suspicious customer activity



Accounts were opened in one of the branches of the Bank of the Kyrgyz Republic for customers OsOO "LTD" and OsOO "LLC" based on the provided legal documents, and Internet banking for legal entities was connected through an authorized person.

Brief details about the companies:



OsOO "LTD" is an organization with foreign participation that was registered as a legal entity in April in accordance with the certificate.

- The company's registered address is Bishkek city, Pervomaisky District.
- Primary activity: No. 46.90.0: Wholesale non-specialized trade.
- Registration with the Tax Service.
- Registration with the Social Fund.
- There is no information available about budget payments.



OsOO "LCC" is an organization with foreign participation that was registered as a legal entity in April in accordance with the certificate.

- The company's registered address is Bishkek city, Pervomaisky District.
- Primary activity: No. 46.90.0: Wholesale non-specialized trade.
- Registration with the Tax Service.
- Registration with the Social Fund.
- There is no information available about budget payments.

Within the framework of implementation of the policy on organizing internal controls for the purpose of anti-money laundering and combating financing of terrorism (hereinafter referred to as AML/CFT), while monitoring the operations of OsOO "LTD" and OsOO "LLC" companies, which were established in April, it was revealed that these companies were related.

Accounts were opened in one of the branches of the Bank of the Kyrgyz Republic for customers OsOO "LTD" and OsOO "LLC" based on the provided legal documents, and Internet banking for legal entities was connected through an authorized person.

Unreasonable account activity

The disproportionately high frequency of transactions compared to previous months raised the bank's concerns. During the verification of previously submitted invoices on delivery terms, contracts, and agreements, inconsistencies and the absence of relevant documents related to **legal contracts with counterparties** were discovered, raising concerns about the legality of economic transactions. Furthermore, all transactions concealed information about the purpose of the money transfers, using phrases such as "for goods," "under contract," or "**auto parts**". After identifying suspicious cases, the Compliance Control Service conducted an internal investigation as part of enhanced customer due diligence to reduce the bank's risks.

Abnormal transaction amounts

Large transfers without a clear economic justification or inconsistent with the customer's financial situation.

Information is kept confidential in accordance with Kyrgyz Republic laws governing banking and commercial secrecy.



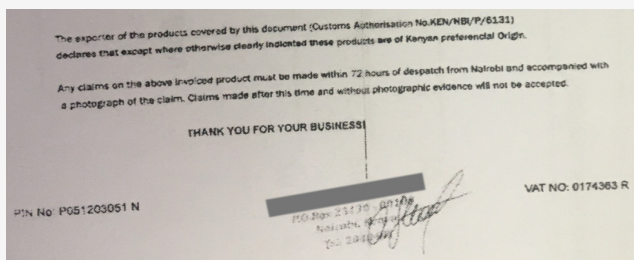
Strange geographic destinations

Receiving funds from CIS countries and sending them to high-risk jurisdictions:

Counterparty from Nairobi, Kenya

The counterparty exports more than 100 types of bush and single-headed roses. The farms are located in Northern Kenya on the slopes of the Great Rift Valley. The roses are grown in greenhouses covering 85 hectares at an altitude of 2,200 meters above sea level, yielding exceptionally high quality T-Hybrid roses. The counterparty exports more than 60 million stems per year to 25 different countries around the world.

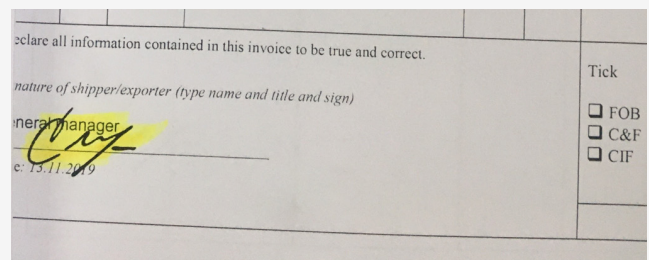
The company's brand is well-known in the floral industry, and it remains a preferred supplier.



However, the company described the purpose of the payments as "for goods" or "textiles".

Counterparty from Panama

According to data from available Internet resources, the company with a similar name exports textile products and provides the corresponding types of services. By type of activity: exporter, manufacturer, supplier. However, there was only a coincidence in the name of the company. It was not found in the Internet resources according to the declared contract or invoice of the customer, which further aroused the bank's suspicion.



The company described the purpose of the payments as "for auto parts", "under contract", or "textiles".

In addition to the aforementioned counterparties, the legal entity's questionnaire included counterparties from seven countries and one individual entrepreneur from the Kyrgyz Republic.

Lack of transparency

The customers failed to provide the required documentation to confirm the sources of funds, posing additional risks. B As part of the implementation of the policy on organizing internal controls for AML/CFT purposes, the Bank has requested the following relevant documents from the customer: all contracts with counterparties, the route of transportation of the goods from the seller to the final recipient, or the agency contract, explanation of transactions with counterparties from Nairobi, Kenya, and Panama, individual entrepreneur's explanation of the contract with OsOO "LTD", certificates of quality of goods indicated as "for fabrics" and "for auto parts" from counterparties in other countries, a statement from the Bank that services the counterparties sending the funds, Bills of Entry, Consignment Notes, Acceptance and Transfer Certificates for goods indicated as "for fabrics" and "for auto parts", agreements and contracts with counterparties from foreign countries.

1. Request of documents

The bank requested a number of documents from the customer to confirm the legitimacy of the transactions.

2. Lack of information







Customers did not provide the required documentation, which raised suspicions.

3. Additional risks

Lack of transparency in transactions created additional risks for the bank.



A brief analysis of customer transactions revealed the following:

-  **Conversion of funds**
The funds received in the settlement account were immediately converted by the customer and transferred to high-risk countries (Panama is an offshore zone)
-  **Power of attorney**
According to the authorized person, the power of attorney was only issued for one month, "to open accounts and connect Internet banking".
-  **General Director**
Despite being a foreign citizen, the General Director is listed as a citizen of the Kyrgyz Republic under the organization's decision.
-  **No registration as a VAT payer**
There is no registration as a VAT payer.
-  **IE(KR)**
The individual entrepreneur (KR) also indicated that he sells textile products in the "Madina" market of the Kyrgyz Republic, as well as products to CIS countries; there is no economic feasibility.
-  **Invoices are inconsistent**
Invoices between the customer OsOO "LTD" and its counterparties are inconsistent with the type of activity of the counterparties, because under the contract, OsOO "LTD" exports auto parts and textile products, and according to information from available Internet resources, the types of activity of the counterparties are different (producers of bush and single-headed rose types, exports of textile products and providing services related to textiles in Taiwan, and exports of cotton, polyester, wool, and knitted fabrics).



Tax payments

A check in the tax base of the Kyrgyz Republic showed that OsOO "LTD" did not pay taxes in 2019 and 2020. According to the Kyrgyz Ministry of Finance's website (<https://budget.okmot.kg/>), the company paid KGS 932 in taxes to the budget for certificate registration, re-registration, and garbage collection.



Founder/Director

The customer (founder and director) used Internet banking to make SWIFT payments without visiting the bank. Account replenishment and withdrawals were carried out by representatives and other officials who are residents of the Kyrgyz Republic. According to the branch employee, the founder/director does not reside in Kyrgyzstan.



Absence of the company at the place of registration

OsOO "LTD" is not present at the registration location..



No quality certificates

Counterparties do not provide quality certificates for "auto parts" products.



Explanation on the transactions with counterparties

According to the explanation of transactions with counterparties, the company's business is to supply bush and one-headed roses, as well as knitted fabrics (Taiwan).

Детальное поступление по платежам
Область с ограниченной ответственностью [redacted]
С 01.01.2019 по 31.12.2019

№ документа	Дата	Платеж	Назначение платежа	Сумма
44000000	25.01.2018	0500	За регистрацию на Ю-40000000	410,00
23040000	25.04.2018	0500	За регистрацию на Ю-40000000	410,00
23040000	24.05.2018	0500	За регистрацию на Ю-40000000	112,00
Итого:				932,00

Итого 932,00. Удостоверенный п.с.

Besides that, a related company was discovered, operating under a similar scheme and registered in April for the same type of activity (wholesale non-specialized trade), with foreign participation of the companies' managers and founders, raising further concerns about the legality of the transactions. The customer's actions called into question the legitimacy of the previously provided documents, as well as the scheme for receiving funds from other countries in the Kyrgyz Republic and sending them to other jurisdictions. It is possible that the companies were formed as shell companies with the goal of legalizing (laundering) criminal proceeds.



Financial transactions

Suspicious financial transactions involving conversion and transfer of funds.



Legitimacy

Doubts about the legitimacy of companies and their transactions.



Registration date

Companies are registered in the same month, raising suspicions.



Geographic destinations

Transfers of funds from CIS countries to offshore zones.

The Compliance Control Service sent an official request through the branches of the Bank and suspended the customer's activities until all relevant documents, contracts, specifications, etc. are provided, based on Article 21, paragraph 1, 4 of the Law of the Kyrgyz Republic on Combating the Financing of Terrorist Activities and Legalization (Laundering) of Criminal Proceeds, paragraph 12, subparagraph 6 of the Regulation on the Customer Due Diligence Procedure (approved by Government Decree No. 606 dated December 25, 2018) and the previously concluded agreement with the Bank under clause 2.2.2 of the agreement on opening and maintaining bank accounts.

As part of the implementation of the policy on the organization of internal controls for AML/CFT purposes, the customer has been requested to provide the following documents:

All contracts with counterparties to whom the purchased goods will be sold, as well as for previously performed transactions according to invoices

The route of transportation of the goods from the seller to the final recipient, or the agency contract

Explanation of transactions with counterparties from Nairobi, Kenya, and Panama related to the supply of various types of bush and single-headed roses, exporting textile products and providing textile services in Taiwan, as well as exports of cotton, polyester, wool, and knitted fabrics

A statement from the Bank that services the counterparties sending the funds

Agreements and contracts with counterparties from foreign countries

Bills of Entry, Consignment Notes, Acceptance and Transfer Certificates for goods indicated as "for fabrics" and "for auto parts"

Individual entrepreneur's explanation of the contract with OsOO "LTD" including supporting documents, such as "video and photos from the market 'Madina' on the sale of fabrics"

Certificates of quality of goods indicated as "for fabrics" and "for auto parts" from counterparties in other countries

Furthermore, according to foreign countries' "On Contracts" laws, the contract must be concluded in writing. Taking into account the norms of law of partners, the norms of law of the UN Convention on Contracts for the International Sale of Goods, as well as the Civil Code of the Kyrgyz Republic, according to which transactions in writing must be made by drawing up a document expressing its content and signed by the person or persons making the transaction, the execution of a foreign trade contract shall be carried out in writing in order to ensure cooperation and legality of the sale or purchase of goods and to protect the parties of the counterparty and the customer from further discrepancies.

The contract shall include the following sections:

1. Name of the parties or surname, name and place of residence of the counterparty

6. Term of delivery of goods, choice of delivery, place, and method of contract fulfillment

2. Subject of the contract for the supply of goods

7. Product warranty obligations

3. Quantity of products to be supplied

8. Liability for non-fulfillment of the foreign trade contract and applicable law

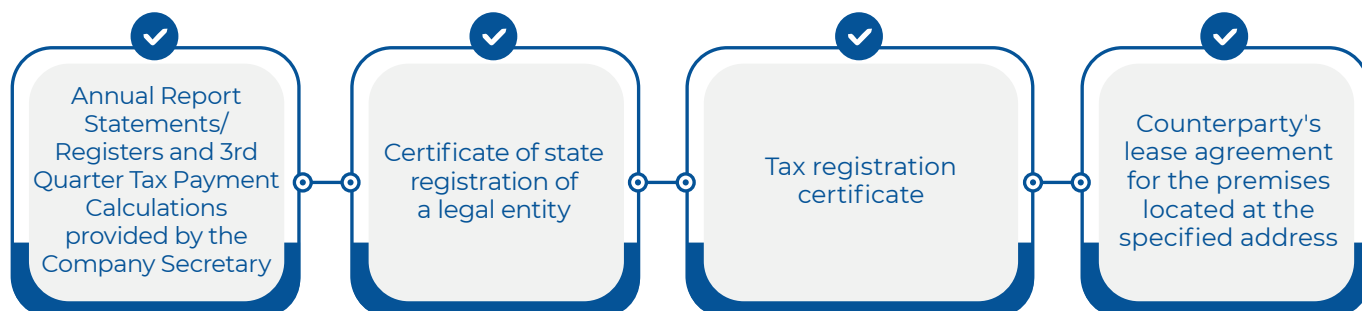
4. Quality of goods, including availability of the certificate of product quality

9. Dispute settlement methods, claim procedure and consideration of the dispute in court

5. The cost of goods, including per unit, as well as the currency of future payments and, if necessary, its conversion

The contract on delivery of goods is fulfilled not only by delivering and paying for the goods in accordance with the terms of the foreign trade contract, but also by executing all necessary documents, including customs, and paying customs duties and fees. When conducting foreign trade operations, it is directly prescribed to draw up a supply contract, i.e. *"the absence of a contract is a violation not only of Kyrgyz Republic legislation, but also of legislation of other countries."*

In addition to the above request, they asked the **Company Secretary to confirm in writing** that the company was not established as an offshore company or is not an offshore company in a foreign country – according to the country's laws, every company must have a secretary in its structure, in addition to a director and shareholder. A company secretary is a legal or natural person who must be a resident. It is important to note that a **Company Director cannot be a Company Secretary**.



Importance of documents

1. Legislation

According to foreign countries' "On Contracts" laws, the contract must be concluded in writing.

2. UN Convention

Taking into account the norms of law of partners, the norms of law of the UN Convention on Contracts for the International Sale of Goods, as well as the Civil Code of the Kyrgyz Republic, according to which transactions in writing must be made by drawing up a document expressing its content and signed by the person or persons making the transaction, the execution of a foreign trade contract shall be carried out in writing in order to ensure cooperation and legality of the sale or purchase of goods and to protect the parties of the counterparty and the customer from further discrepancies.

3. Protection of the parties

The execution of a foreign trade contract shall be carried out in writing in order to ensure cooperation and legality of the sale or purchase of goods and to protect the parties of the counterparty and the customer from further discrepancies.

Suspicious transactions

1/ Non-compliant documents

During the verification of CPT invoices, contracts, and agreements for opening and maintaining bank accounts, the customer failed to provide all requested documents or was unable to respond and prove the legitimacy of the companies' activities.

2/ Complex scheme for the movement of funds

These customer actions raise concerns about the legitimacy of previously submitted invoices. There is a complex scheme of receiving funds from other countries in the Kyrgyz Republic and sending funds to other countries with the purpose of payments indicated as "for fabrics" and "auto parts".

3/ Suspicion of money laundering

The nature of the transactions or circumstances raises the possibility that they were carried out with the intent of legalizing (laundering) criminal proceeds. Moreover, the signatures of managers differ from the previously submitted samples; signatures in contracts are likely to be forged, raising further concerns about the legality of the customer's transactions.

4/ Illegal practices

The company's transactions may reveal illegal or unethical practices, such as money laundering, tax evasion, financing of terrorist or illegal activities, fraud, or other predicate offenses.

4/ Illegal financial transactions

Suspicious may be based on a variety of factors, such as illegal financial transactions, suspicious cash flows, a lack of documentation, non-compliance with the "On Combating the Financing of Terrorist Activities and Legalization (Laundering) of Criminal Proceeds" law, or other requirements.

6/ Forgery of signatures in contracts

Forgery of signatures in contracts is a serious offense that can result in criminal charges. This act is typically classified as fraud or forgery of documents. Most countries impose stiff penalties, such as fines and prison sentences.

7/ Dubious contracts

The customer provided the agreements and contracts that serve as the foundation for the transactions. However, the manager's signature in the agreements and contracts differed from the previously submitted samples; the content of the contracts is also questionable; all of the submitted contracts may have been prepared using the same template.

The customer's AML/CFT risk assessment revealed the following indicators of suspicion:

Suspicious may be based on a variety of factors, such as improper financial transactions, suspicious cash flows, a lack of documentation, non-compliance with the "On Combating the Financing of Terrorist Activities and Legalization (Laundering) of Criminal Proceeds" law, or other requirements. The company's transactions may reveal illegal or unethical practices, such as money laundering, tax evasion, financing of terrorist or illegal activities, fraud, or other predicate offenses:

The customer provided the agreements and contracts that serve as the foundation for the transactions. However, the manager's signature in the agreements and contracts differed from the previously submitted samples; the content of the contracts is also questionable; all of the submitted contracts may have been prepared using the same template. Besides that, in all contracts entered into by OsOO "LTD," the full name of the General Director of related company, OsOO "LLC," is erroneously indicated. The contracts do not specify the name, quantity, or cost of the goods to be supplied. There are no other documents confirming the reality of purchase and sale under these contracts. In the electronic version of the contract provided, when you hover over the signature of Mr. Jameson (Panama), there is a link https://upload.wikimedia.org/wikipedia/commons/2/20/Sergey_Mylnikov_signature.svg to the signature of Sergei Mylnikov, a USSR hockey player who died on July 20, 2017.



***Sergey Mylnikov is an Honored Master of Sports of the USSR, goaltender, "Tractor" (Chelyabinsk)**



Sergei Mylnikov was born on October 6, 1958, in Chelyabinsk. Many times he defended the gates

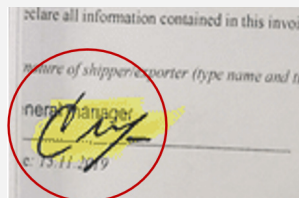
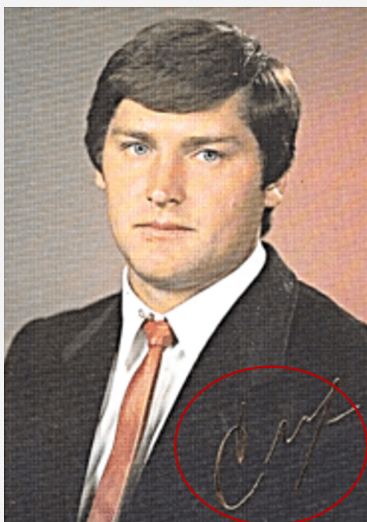
of the national teams: junior, youth, and second national team. Showing a confident game, he often helped the team in difficult situations.

Sergei was 26 years old when he joined the USSR national team. He and Vladimir Myshkin replaced Vladislav Tretiak, the outstanding goaltender.

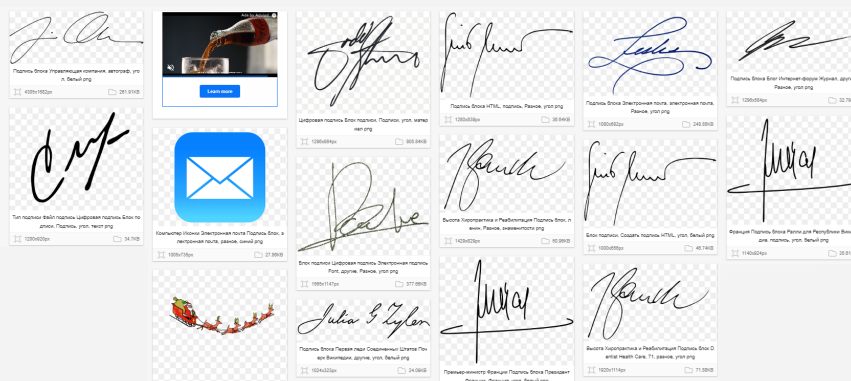
Mylnikov's outstanding sportsmanship and dedication to hockey were on full display at the Olympic Games tournament in Calgary, where he consistently defended the USSR national team's gates.

Sergei would play for the Quebec Nordiques of the National Hockey League in the 1989-90 season.

Sergei Mylnikov received the Order of the Badge of Honor for his contributions to Soviet hockey.



We also suspect that other documents confirming the reality of the purchase and sale under these contracts may be forged and copied using Internet resources such as digital PNG signatures in Google



During the verification of CPT invoices, contracts, and agreements for opening and maintaining bank accounts, the customer failed to provide all requested documents or was unable to respond and prove the legitimacy of the companies' activities. These customer actions raise concerns about the legitimacy of previously submitted invoices. There is a complex scheme of receiving funds from other countries in the Kyrgyz Republic and sending funds to other countries with the purpose of payments indicated as "for fabrics" and "auto parts". The nature of the transactions or circumstances raises the possibility that they were carried out with the intent of legalizing (laundering) criminal proceeds. Moreover, the signatures of managers differ from the previously submitted samples; signatures in contracts are likely to be forged, raising further concerns about the legality of the customer's transactions.

According to the analysis of the customer's activities by the compliance control service, the transactions were classified as suspicious and reported to the State Financial Intelligence Service (SFIS) under the Ministry of Finance of the Kyrgyz Republic:



Additional measures

In addition to the above measures, it is recommended that additional investigation be conducted to obtain more information about the activities of the customers OsOO "LTD" and OsOO "LCC". This may include reviewing financial records, interviewing the customers and their counterparties, and cooperating with law enforcement agencies.

- ✓ non-cash transfers of funds by resident bank customers in favor of non-residents (particularly in cases where the jurisdiction of the non-resident counterparty under the contract does not coincide with the jurisdiction of the non-resident bank where the non-resident counterparty's account is opened);
- ✓ the customer's strong desire to work independently from a remote terminal; the customer's desire not to enter into personal contact with the bank or other financial and credit institutions, including through the use of representatives (intermediaries) and means of communication (Internet, mail, telephone, fax, etc.), allowing the customer to transmit orders to carry out operations (transactions) without direct contact with the bank or other financial and credit institutions;
- ✓ non-standard or unusually complex settlement instructions that differ from the normal practice used by that customer or the normal market practice;
- ✓ other circumstances that give grounds to believe that transactions are carried out for the purpose of legalizing (laundering) proceeds of crime;
- ✓ significant changes made by the customer to the previously agreed scheme of the operation (transaction) immediately before its realization, especially in terms of the direction of cash flow or other property;
- ✓ the unclear or unusual nature of a transaction (deal) that has no obvious economic sense or obvious legitimate purpose;

- ✓ difficulties encountered by reporting entities in verifying the information provided by the customer, unreasonable delays in the provision of documents and information by the customer, and the provision of information by the customer that cannot be verified or is too costly to verify;
- ✓ non-compliance of a transaction (deal) with the objectives of the organization's activity established by this organization's constituent documents;
- ✓ transferring funds by a resident to non-residents registered in an offshore zone;
- ✓ receipt of funds by a resident from entities registered in an offshore zone;
- ✓ if at least one of the transaction's parties is a natural or legal person registered, residing, or located in an offshore zone, or if one of the parties has an account with an offshore zone-registered bank.



Taking into account the foregoing, the Compliance Control Department believes that the Bank's customers OsOO "LTD" and OsOO "LLC" may be engaging in false entrepreneurial activity and transferring funds through the Bank for the purpose of money laundering.

Based on Article 21 of the Kyrgyz Republic's Law on Combating the Financing of Terrorist Activities and the Legalization (Laundering) of Criminal Proceeds, we recommend that the Bank's Management Board unilaterally terminate business relations with the customers OsOO "LTD" and OsOO "LCC" by closing all accounts and blacklisting the customers.



In accordance with the banking and commercial secrecy,

Law of the Kyrgyz Republic on Combating the Financing of Terrorist Activities and Legalization (Laundering) of Criminal Proceeds No. 87, dated August 6, 2018, "company names, dates, and persons in the material are anonymized to protect the confidential information of the Bank, SFIS, and other law enforcement agencies.

Attack in the digital world: phishing, carding and cryptocurrency money laundering schemes

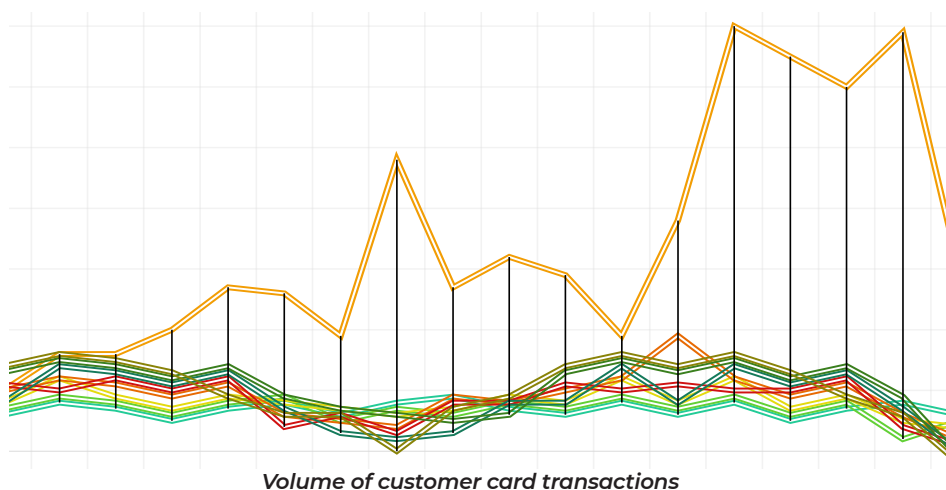
Mr Khurram Rizoiev, Senior officer of compliance service of CJSB "International bank of Tajikistan", Republic of Tajikistan

Analysis and initiation of detection

Here is a detailed analysis of an incident involving suspicious activity detected by monitoring systems. This case is a prime example of how modern technologies such as Tableau enable timely detection of anomalies in financial activity.

Incident Description

The incident began with a sharp increase in transfers and turnover on the accounts of a customer named Rustam. At the same time, a notification was received from VISA about suspicious activity related to more than 70 P2P transactions made in one day. Monitoring systems showed atypical activity, which allowed an investigation to be launched.



Phase A: bank card data collection (phishing and carding)

In the first phase of the investigation, it was determined that the attackers used phishing schemes to collect bank card data. In this case, UAE cardholders were the primary targets. The criminals used social engineering techniques, including fake websites and fake messages,

Key Indicators (Red Flags):

Sharp increase in transfers and account turnover.

Client Rustam significantly increased the volume of transactions in a short period of time, which did not correspond to his previous financial activity.

Massive number of P2P transactions.

More than 70 transactions in one day is a clear deviation from the norm, especially for this client.

Notification from VISA.

A report of suspicious activity initiated by an external payment system also prompted a detailed analysis.

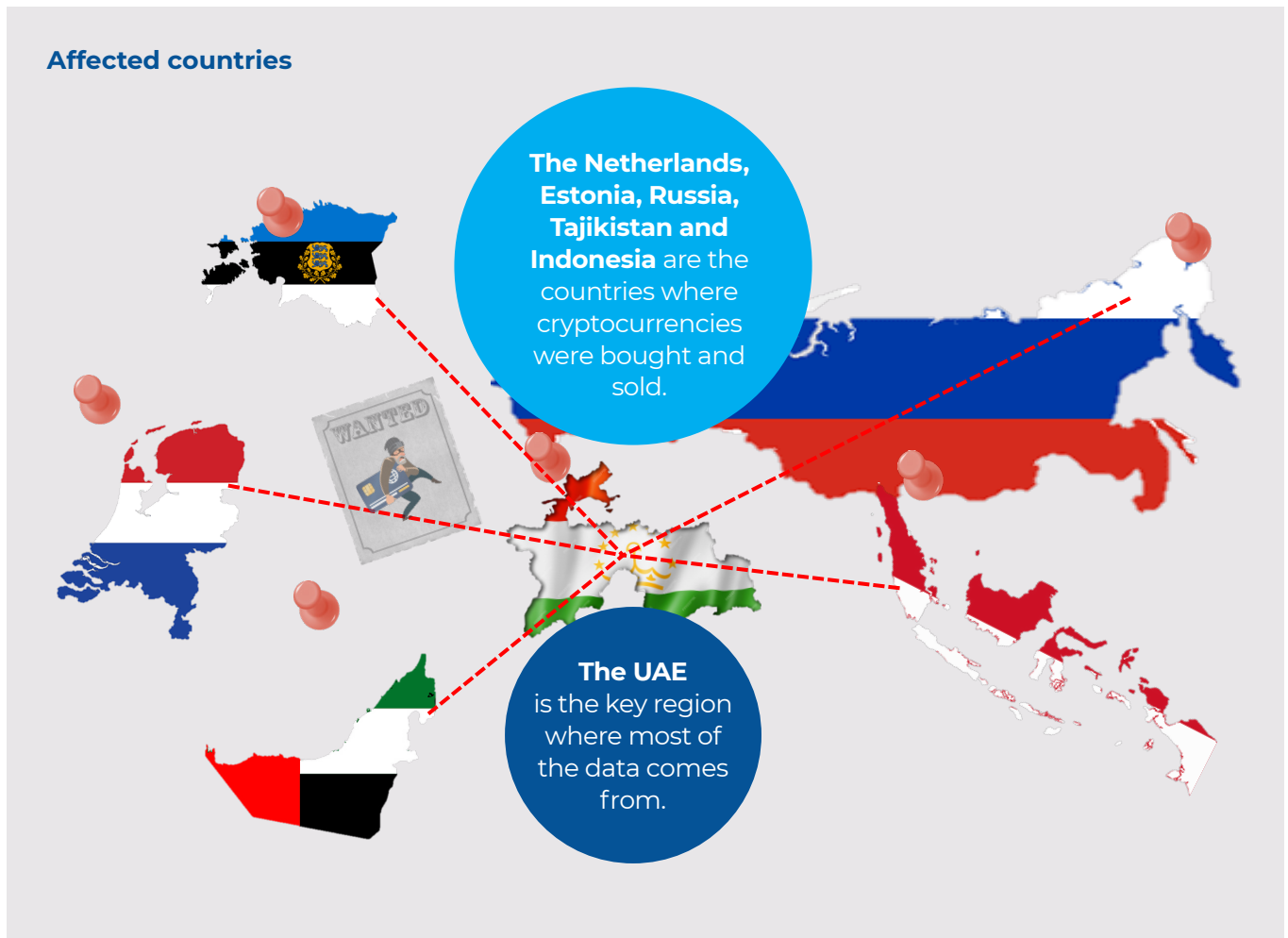
Detection of suspicious activity in several systems.

Comparison of data from different sources confirmed suspicions.

Atypical financial activity of the client.

The combination of all these signs indicated possible illegal activities that required further investigation.

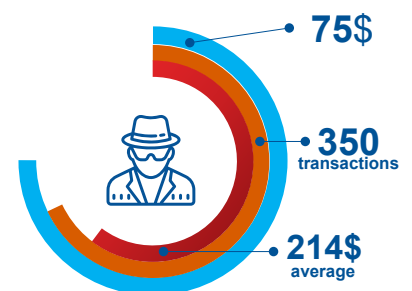
to trick victims into providing sensitive information such as card numbers, CVV codes and other sensitive data. The use of such techniques is typical of phishing attacks, where attackers pretend to be official institutions or companies. This data was later used for illegal operations such as carding.



Phase B: using data for cryptocurrency transactions

The next stage of the investigation revealed that Rustam used the stolen card data to purchase cryptocurrency. The carding process involved buying cryptocurrency through online platforms and then transferring it to anonymous accounts. In order to cover his tracks, he used several methods:

- **Smurfing:** Funds were split into small amounts and sent to different accounts to hide their origins and make them harder to trace.
- **Mixers:** Special services that “mix” cryptocurrency transactions from different users, making the process of tracing the sources of funds nearly impossible. This stage of fraud is critical to legalization of funds, as cryptocurrency transactions are harder to trace compared to regular bank transactions.

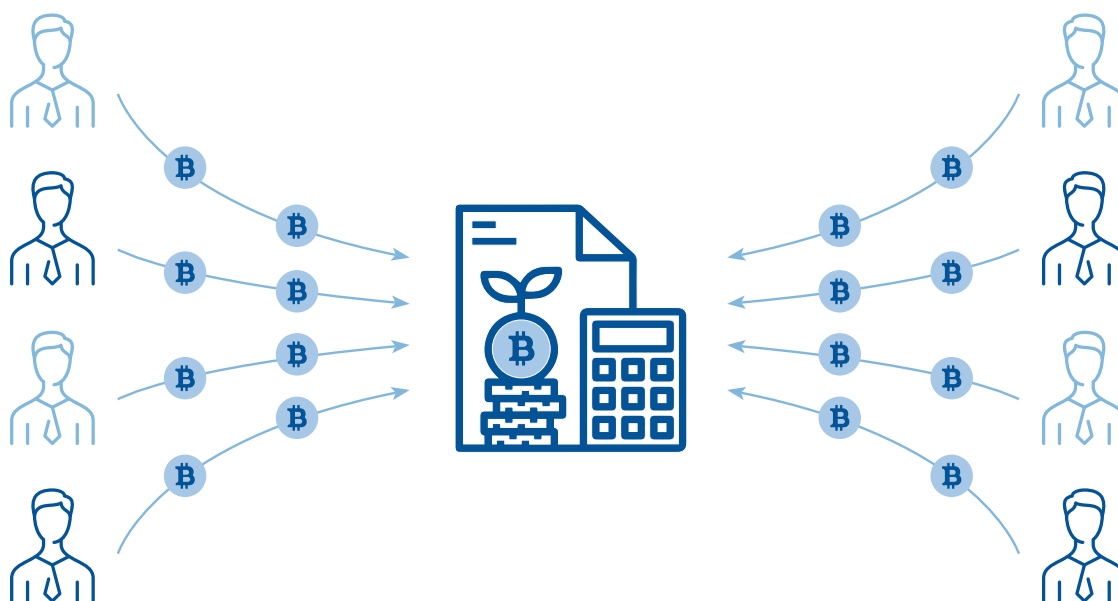


>70,000 USD

the total damage from Rustam's offences, according to preliminary data

Phase C: cryptocurrency arbitrage and fundraising

Rustam's next step was cryptocurrency arbitrage. He used the difference in exchange rates between different crypto exchanges to make a profit. In short, it looked like this: he bought cryptocurrency on one platform at a low price and sold it on another at a higher price. In this way, Rustam made profits through arbitrage. To increase capital and maximize profits, he raised funds from third parties, promising them a share of the profits. This allowed him to participate in larger transactions while concealing the true source of the funds, as the third-party investors disguised the origin of the money.



Countermeasures against suspicious transactions

1/ Identifying transaction anomalies

We have implemented more proactive monitoring systems that automatically identify atypical financial transactions.

2/ Freezing of funds

In case of detection of suspicious transactions and confirmation of anomalous activity on the client's accounts, we have implemented a mechanism for instant freezing of funds.

3/ Strengthening control over high-risk clients.

We have improved the system of classifying clients by risk level.

4/ Notification of clients.

In cases of suspicious activity, we immediately notify clients of possible risks.

5/ Transaction monitoring.

Implementation of 24/7 transaction monitoring using advanced algorithms.

6/ Increasing the level of account security.

We implemented additional mechanisms for authentication and protection of customer accounts.

7/ Partnership with the Department of Financial Monitoring.

Effective sharing of information on suspicious transactions with government regulators.

Phase D: withdrawal of funds via mobile wallets

At the final stage of the scheme, Rustam redistributed the funds through a network of mobile wallets. Each wallet would receive a transfer from the previous one, then pass the funds on. This chain of wallets made tracking transactions much more difficult, as each step added an additional layer of confusion. Final legalization: eventually, the stolen funds were withdrawn to bank accounts. This is how Rustam, using phishing, carding and cryptocurrency arbitrage, legalized the stolen money, hiding the traces of his criminal actions.



Actions after analysis: from assessment to implementation of solutions

The analysis revealed clear inconsistencies and anomalies in the transactions indicating their suspicious nature. Indicators such as unusually large amounts, high frequency of transactions and the use of non-transparent counterparties confirmed the need for further investigation. Based on the findings, the transaction was categorized as suspicious. We sent a Suspicious Transaction Report (STR) to the Financial Monitoring Department under the National Bank of Tajikistan for additional checks. In response to the information provided, the Financial Monitoring Department recommended freezing the funds on the suspicious accounts. As a result of these actions, over USD 12,000 was frozen, preventing further movements of funds and reducing the risks of financial irregularities.



This incident emphasizes the importance of timely detection of anomalies in financial activities and the use of modern technology to prevent financial crime.

Case 8

Tax Avoidance Scheme via consumer cooperative terminals installed at dental chain clinics

Mr Aleksandr Popov, Director on financial monitoring and compliance
of the PJSB Rosbank, Russian Federation

General Information on the NPO Industry and Statutory Regulation

Domestic regulation

- **Civil Code:** a consumer cooperative (CC) – is a NPO entity
- **Tax Code:** funds provided to NPO entities are tax-exempt

FATF recommendations on NPO entities

- Address the risk of concealing the sources under the guise of donations, FT and siphon funds off to high-risk countries
- The recommendations are not related to the identified tax avoidance scheme

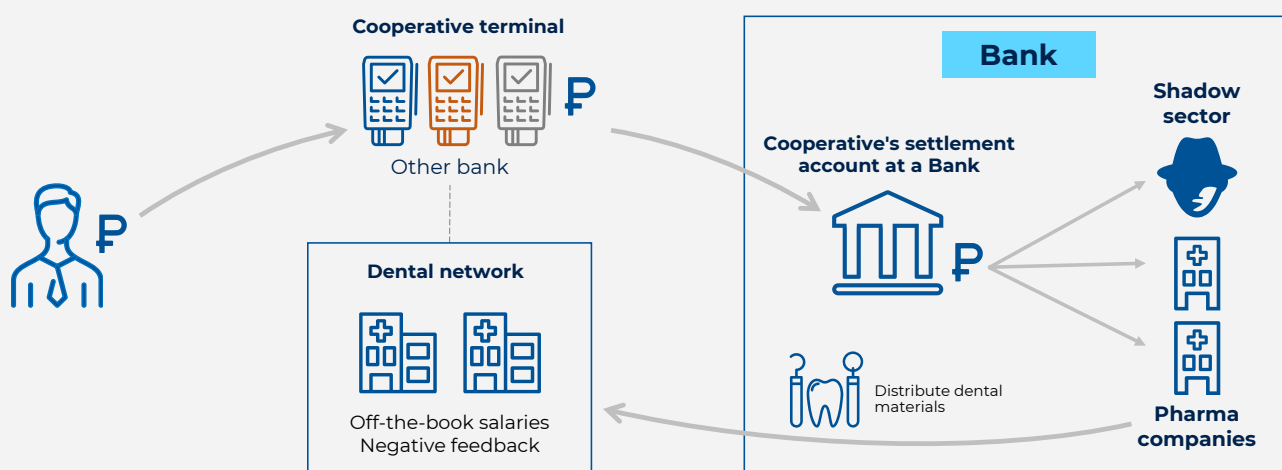
Russian market
review annually

+10 000
NPO entities

The overall tally is

> 225 000
NPO entities

Tax Avoidance Scheme Using Consumer Cooperative Infrastructure



Fact: acquiring proceeds

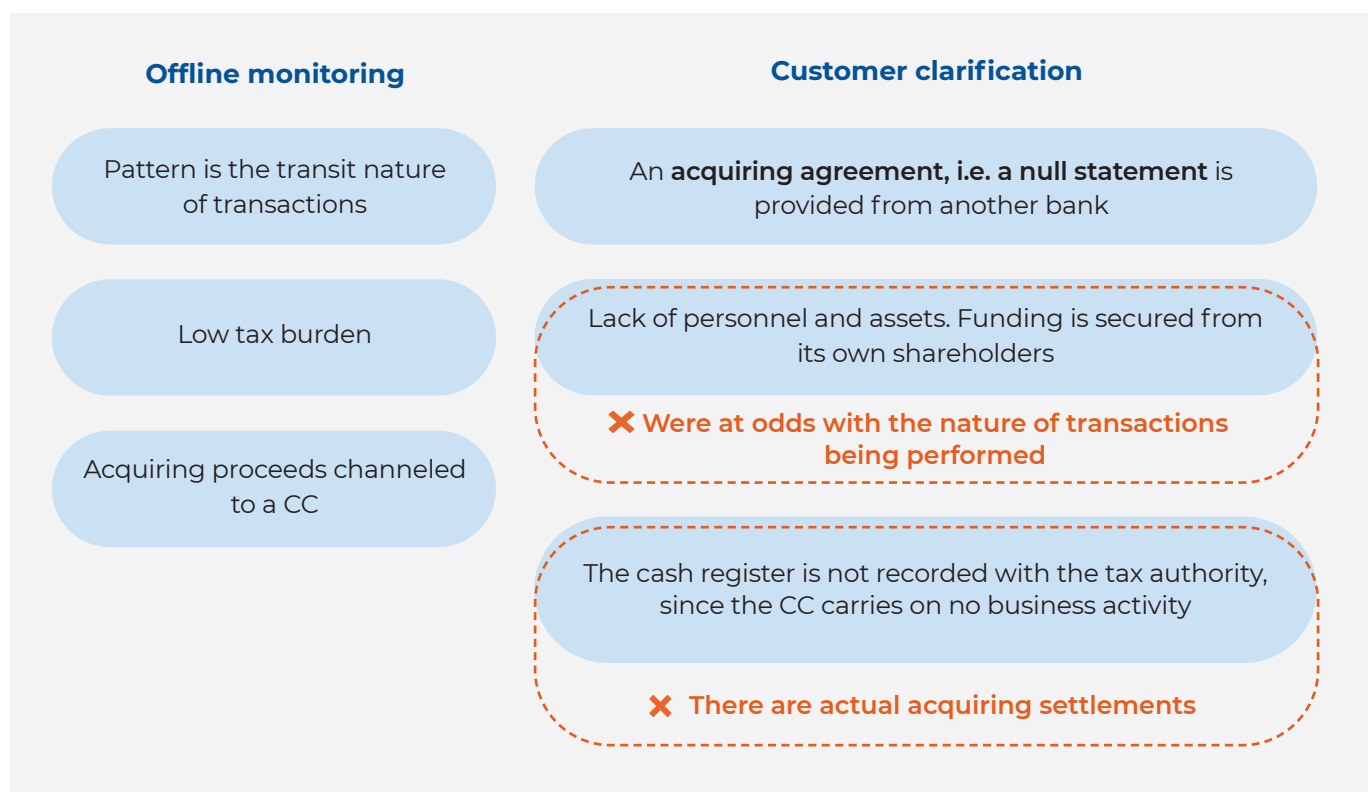
Contributions directly paid by shareholders

Fact: transfer of funds to an entity – pharmaceutical companies

The cooperative should cater to the needs of the shareholders

Fact: payments are at odds with the CC goals

Scheme Identification



Specific Scheme Aspects



Proceeds from another bank under an acquiring agreement



Reference to the dental clinics in incoming payments



Transactions were at odds with the nature of the CC business



Outgoing payments for dental supplies



At installation points of terminals - dental clinics



Negative feedback from the personnel on social media

What's been done?

- Customers' transactions were classified as suspicious
- A large-scale investigation was conducted targeting all NCO customers with proceeds both from other banks and from the bank's partner company under an acquiring agreement
- No new schemes were identified

Seen through to completion

- A news scenario was put in place in monitoring tools (online and offline), i.e. funds credited to NPO accounts at the Bank under an acquiring agreement and an ongoing investigation

Scaling

- Reports were submitted to Rosfinmonitoring resulting in recommended practice 66-T being issued

Recommendations for Lending Institutions



Keeping track of amounts
under acquiring agreement
to NPOs' settlement accounts
with following settlement
transactions



**Ensure that the assigned
Merchant Category code
matches the customer's
declared business**
(Recommendations of the Bank
of Russia 13-MR)



Request details
of acquiring transactions



**Ensure that the declared
business activities and
calculations made check out**

Assessment of the potential impact on the financial and economic sustainability and the social domain

Tax avoidance and lower
government revenue

Potential use of NPO accounts for
other purposes, i.e. ML/FT (cashing
out and corrupt practices)



