EURASIAN GROUP CONTEST AMONG COMPLIANCE SPECIALISTS FROM FINANCIAL INSTITUTIONS OF EAG MEMBER STATES FOR THE BEST AML/CFT FINANCIAL ANALYSIS

THE EURASIAN GROUP ON COMBATING MONEY LAUNDERING AND FINANCING OF TERRORISM (EAG)

2022

Content

In Dushanbe, during the 37th EAG Plenary Meeting, an award ceremony was held for the winners and laureates of the first EAG Contest among financial institutions for the best AML/CFT financial analysis and risk profile example

The contestants presented to the contest committee the analytical work of the AML/CFT compliance units in identifying suspicious activities. The contest materials were presented on the margins of the II International Financial Security Olympiad. The students communicated with the experts of the EAG member-states banks, got acquainted with the work of compliance services to mitigate risks.

According to the decision of the contest committee, the winner of the competition became the bank, which had prepared an investigation of illegal online casino activities. The laureate became the credit institution that presented cases on illegal migrants and lending backed by smuggled gold. Based on the results of the student vote, the bank that presented the case of illicit cross-border transfer of funds using foreign trade contracts was declared the winner of the Public Choice Award.

EAG Chairman Yury Chikhanchin noted that the contest is unique and not held in other regional groups. "The winners have shown that the banking system in their countries operates according to the standards defined by the FATF and accepted by the international community. This once again confirms that the national anti-money laundering system is at a high level," stressed the EAG Chairman.

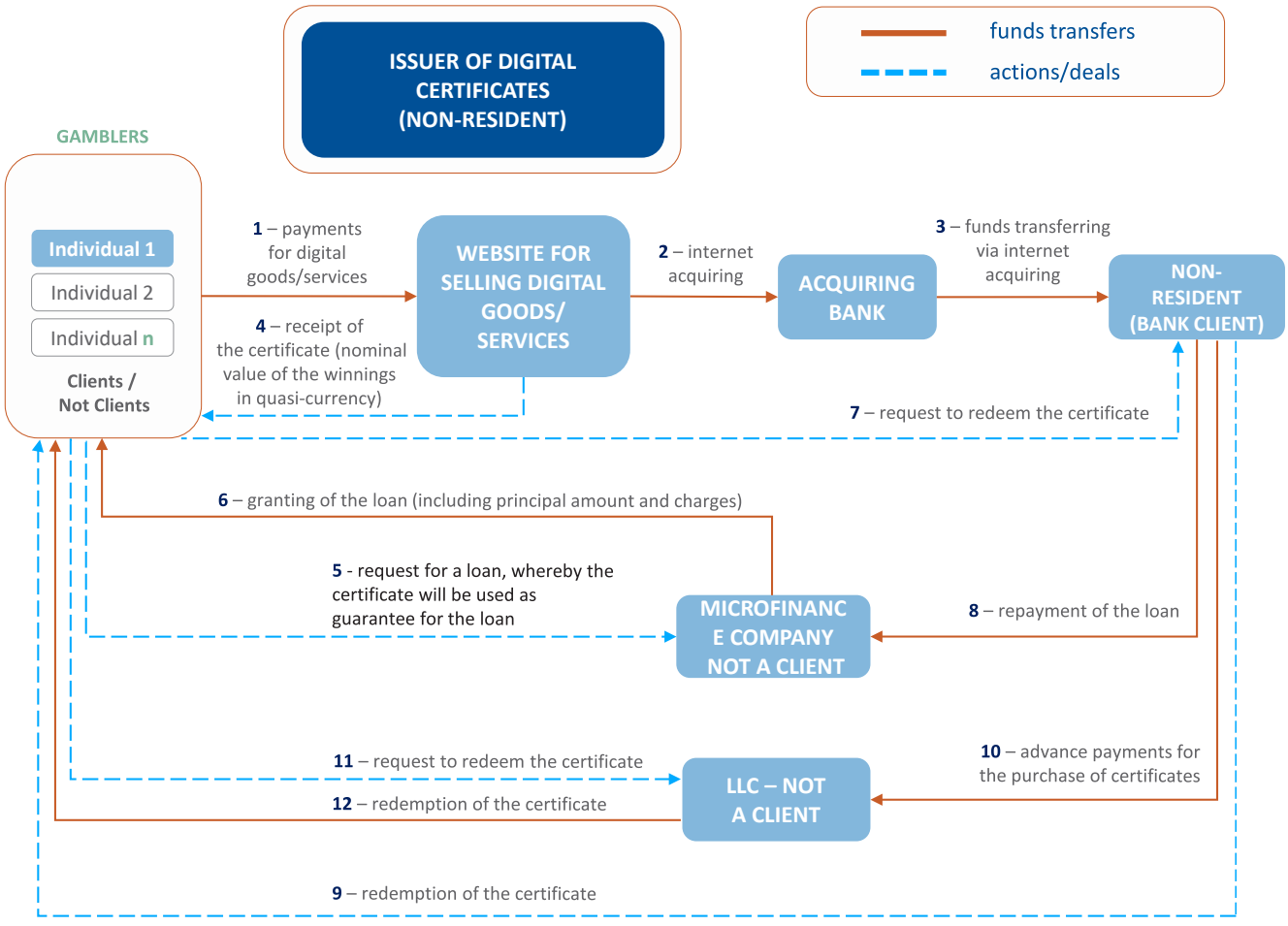
The event is intended to stimulate the dissemination of best practices within the professional community of the Eurasian region, as well as the promotion of public-private partnerships in the anti-money laundering sphere.

Case 1

Withdrawal from an online casino platform

DESCRIPTION: The ongoing monitoring identified a **scheme** of operation by a foreign entity whose real purpose was to participate in the **withdrawal of funds** from an **online casino platform.**

THE **WEBSITE** IN THE INTERNET FOR BUYING AND SELLING DIGITAL GOODS IS USED AS A «FRONT/SHELL» WEBSITE FOR THE **ONLINE CASINO**.



The acquiring bank accepts payments from individuals for sold goods and then transfers the received funds to the customer's account. We believe that, in fact, these transactions represent betting in an online casino. According to the documents, the transactions by payment cards on the website are carried out non-stop, the daily amount varies from 4 to 5 thousand. The funds are received from many individuals in small amounts (from 0,026$ to 105$).

On the day of winning, the individual receives on the website an impersonal digital certificate with the nominal value of the winnings specified in conventional units, and on the same day applies to the microfinance company for a loan by presenting the digital certificate as collateral (in fact, for the receipt of the winnings). On the same day, the microfinance company issues the loan to the individual.

The individual then sends an application to the non-resident client requesting repayment of the certificate. The client, in turn, pays for the certificates received by transferring funds to the details specified by the individual, that is, to the microfinance, towards the repayment of the individual's loan. Approximately 60% of the funds are withdrawn by the client through this chain of actions and settlements.

Also, in order to purchase certificates (namely, to pay out the winnings) the client may use other options, for example:

- transfer the funds directly to the bank account (card) of that individual (certificate holder), but these transactions are likely to immediately come to the attention of compliance services, and this method of withdrawal is used only in 15% of cases;
- transfers money to a third-party agent under an agreement under which the agent buys certificates from individuals on behalf of and at the expense of the client, paying the individuals for the cash advance payment from the client (we assume that also including a service fee), and this withdrawal method is used only in 20% of cases.

The redemption of these certificates makes no apparent economic sense for the client himself, as he is not the issuer of these certificates. We believe that the profit of the client is the money received in the form of bets from individuals who have not won. That is why, according to the documents, the redemption of certificates is carried out from fewer individuals, but for larger amounts.

Thus, the website for the purchase and sale of digital content is used as a kind of "screen" for the illegal activities of online casinos.

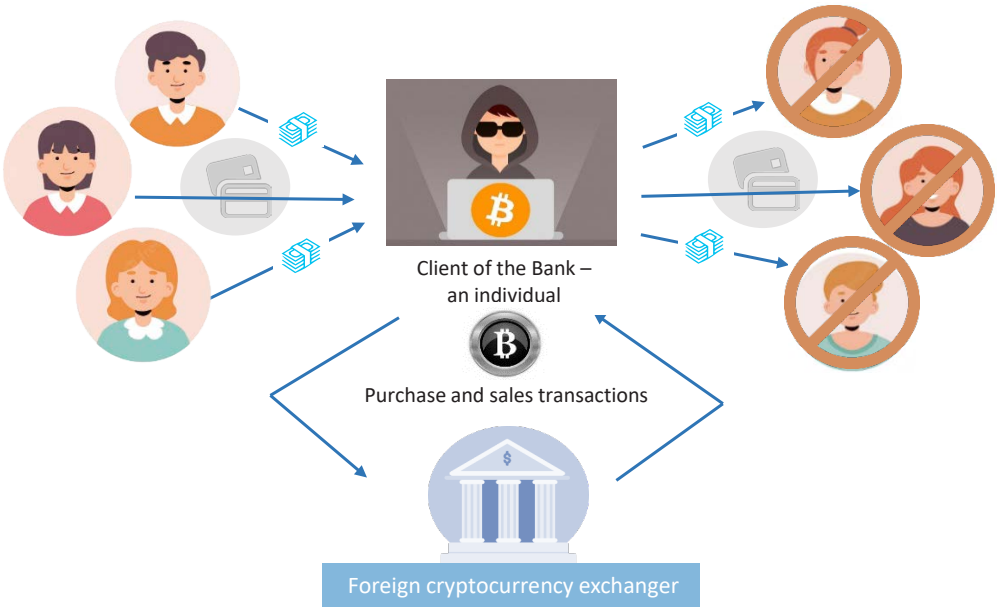
Case 2

Scheme of financial transactions using tokens

DESCRIPTION: conducting a financial transaction by a customer involving the purchase or disposal of tokens for national/foreign currency and electronic money from non-residents for the benefit and/or on behalf of third parties without registering the client as a licensed virtual asset service provider (VASP).

PERFORMANCE OF P2P REMITTANCES BY THE CLIENT THROUGH A FOREIGN CRYPTOCURRENCY EXCHANGER FOR THE BENEFIT AND/OR ON BEHALF OF THIRD PARTIES WITHOUT REGISTERING THE CLIENT AS VIRTUAL ASSET SERVICE PROVIDERS (VASPS).

CRYPTOCURRENCY EXCHANGER



CHARACTERISTIC FEATURES OF THE SCHEME:

- "round" amounts of transfers;
- split transfer amounts (more than 100 transactions in a month);
- the funds credited, usually the same day, are transferred to a third party or cashed out leaving no balance;
- the purpose of the transfers is missing;
- there is no information about the originator and beneficiary of the transfers.

Based on the current legislation of the Country A, if an individual provides services to third parties on the territory of the Country A to perform token transactions on a foreign cryptocurrency exchange, such activities will be illegal.

Persons who engage in such illegal activities, i.e. buying and selling virtual assets for or on behalf of third parties, while not being a registered virtual asset service provider, are conventionally referred to as cryptocurrency exchanger.

A cryptocurrency exchanger carries out P2P transfers through a foreign crypto-exchange for or on behalf of third parties without registering itself as a VASP. The key participants in this scheme are individuals. The difficulty in detecting this scheme is that the financial transactions corresponding to this scheme do not always lie on the surface.

Often there is no communication with the client, then the Bank may apply restrictive measures such as disabling the remote banking system, blocking the card, or setting the card limit to zero, forcing the client to contact the Bank.

As a rule, the client only provides a screenshot of his personal account in the cryptocurrency exchange and an explanation that he is acting within the national legislation, while documents confirming that he is acting in his own interests and at his own expense are not provided to the Bank.

The Bank explains to the client that he may carry out transactions in a foreign cryptoexchange only in his own interests, after which the Bank decides to recognise the financial transactions as suspicious and include the client in the restrictive list for further control.

Thus, the scheme we have examined is illegal, as it shows that the client is engaged in illegal business activities.

Case 3

Withdrawal of capital and avoiding financial monitoring procedures

DESCRIPTION: Deposit of foreign currency in cash by a group of Individual Entrepreneurs, followed by withdrawal of funds from the country using international contracts. At the same time, there were no documents from the customs authority confirming the fact of delivery of the goods.

STATISTICS

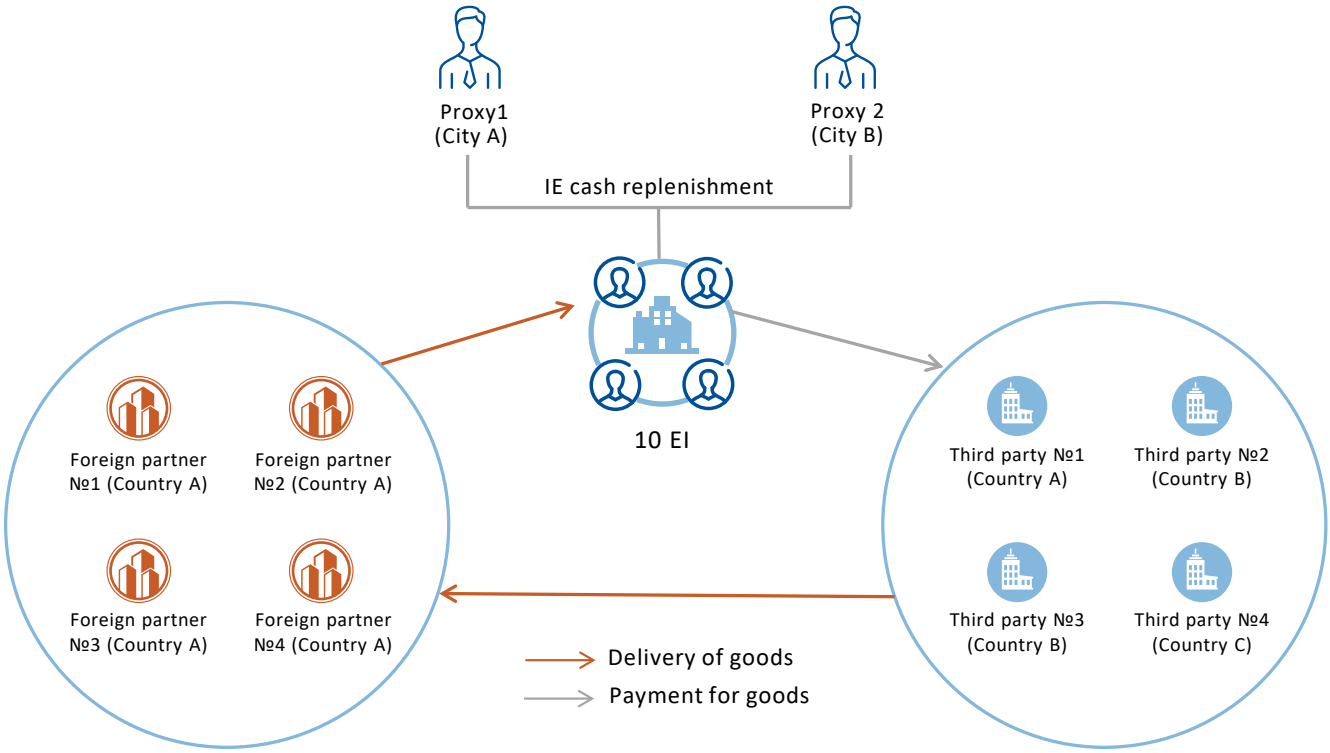
% of the delivery of goods from country A in favor of the individual entrepreneur from the money sent in favor of a third party

30 Average number of contracts with foreign partners for 1 individual entrepreneur

55,2 Average amount in million $ of violations in the supply of goods for 1 individual entrepreneur

90 Average number of additional agreements with third parties at 1 individual entrepreneur

550 Million $ total amount of non-delivery of goods



The initial reason for the in-depth check was to identify a group of individual entrepreneurs (more than 10 individual entrepreneurs) in which funds were managed by 2 proxies and to identify the same counterparties in all of the individual entrepreneurs. The main risk assessment criterion was that the group of individual entrepreneurs had made an unusually large cash deposit transaction into their bank accounts.

In the scheme identified by the Bank, following an in-depth analysis of the transactions of the groups of IEs (individual entrepreneurs), the following factors served as indicators of the risk of money laundering:

- Existence of a very large amount of cash turnover in the group IE's accounts and conversion into foreign currency within a short period of time for subsequent transfer.
- Lack of supporting documents for the source of funds to be used for the financing of the transaction.
- Failure to fulfil obligations under foreign trade contracts by more than 80%, receivables from foreign partners amounted to more than 80%.
- The activity of money transfer within one operational day, more than 10 transfers to different third persons within one contract (one contract involved from 100 to 300 legal entities from different countries).
- In the absence of information on the delivery of goods, a group of IE generates payments in advance to a large number of new third parties, indicating signs of importing goods into the territory of country by smuggling. And it is possible that the group of IEs used an informal financial and settlement system (hawala) for mutual settlements.
- The presence of import contracts that do not provide for the actual receipt of goods on the territory of the country or do not provide for the movement of goods through the territory of country.
- Extension of repatriation deadlines by signing additional agreements.
- Payment in insignificant amounts of taxes or other obligatory payments to the budget.

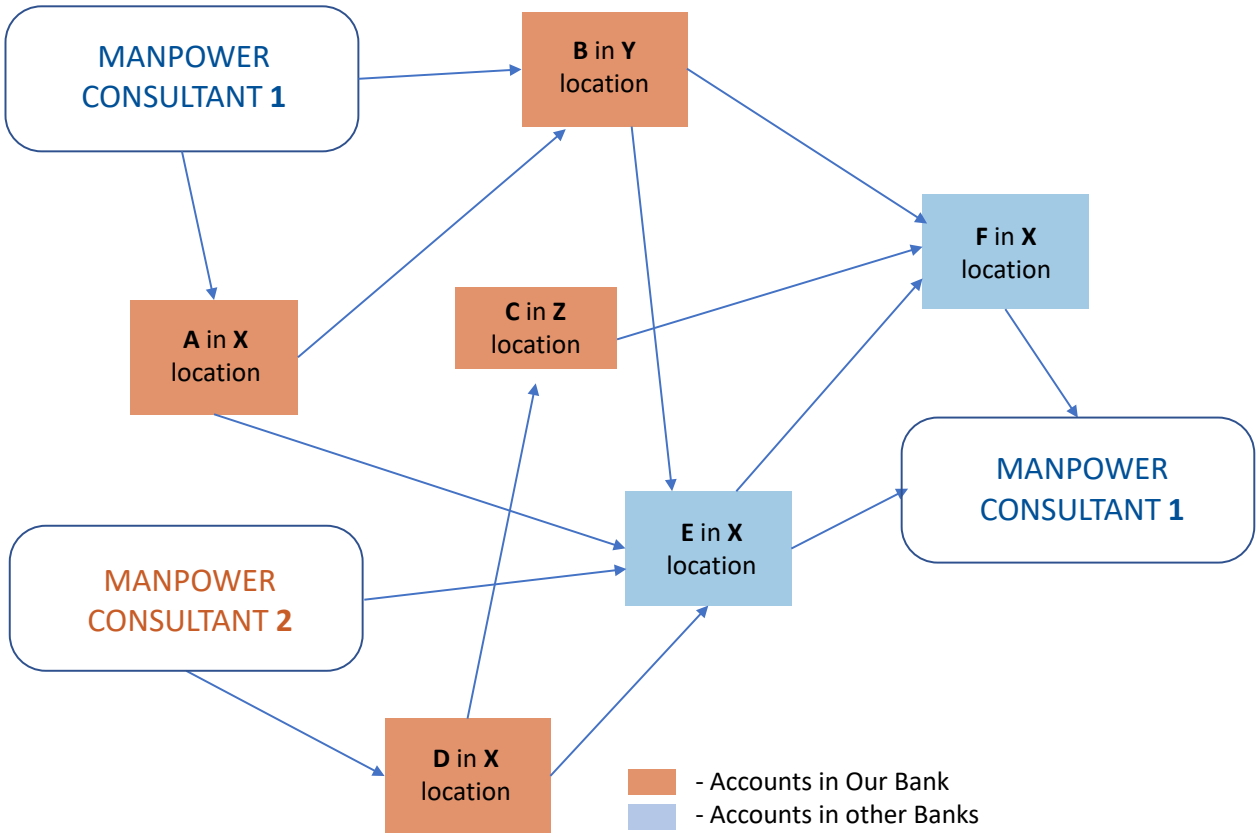
Based on a comprehensive study of the contracts and operations of a group of individuals of IE, the transactions were recognized as a scheme to move capital abroad through foreign economic contracts.

The schemes consisted of a group of IEs crediting their bank accounts with cash and then transferring money under concluded import contracts with counterparties from another country as payment for goods in favour of third parties that were not parties to the contracts on a regular basis. At the same time, there were no documents from the customs authority confirming the delivery of goods. The Bank took measures to suspend the operation, refuse to conduct the operation with further termination of the business and notification of the Authorised Body, in accordance with the requirements of the AML/CFT Law.

Case 4

Money Laundering: Suspicion of human trafficking (illegal migrants)

DESCRIPTION: non-cash deposits in large amounts (from $24000 to $36000) were credited to suspicious accounts **with subsequent transfer of funds** within the bank as well as to other accounts in several banks. The suspicious accounts were opened allegedly to obtain the visa required to pursue studies in foreign universities through employment agents without supporting documents. Suspicious funds related to illegal migration came from employment agents to be laundered through a complex multi-layered structure.



Steep rise in AML alerts pertaining to “Debit or Credit aggregate transaction about 6000 USD and above within 6 months of newly opened Individual account” in particular geographical area of country during July 2021 to February 2022.

Numerous individual savings accounts opened for purpose to create complex layering of funds. These individual savings accounts were opened across 10% of the branches of the geographical area. Accounts opened at branch level (through Tab Banking) in bulk as numbers are in series/ sequence. All accounts are having common attributes such as newly opened individual savings bank accounts in the age group of 18-35 years. The profile of the suspected accounts were mainly students, housewife, service, self-employed and professionals. Few mobile numbers were found linked to almost 1200 such accounts.

All accounts were opened with nominal cash deposit and within a few days high value non-cash funds (ranging between 24000 USD to 36000 USD) were credited in these individual savings bank accounts followed by immediate routing of funds to unrelated parties internally as well as to accounts of other banks. In some accounts Balance certificate was also generated.

After this high valued credit and debit transactions all these accounts stopped having any further transaction and negligible balance was left in the account which raised suspicion. Branches were informed that these accounts were opened for VISA purpose for students who want to pursue study in overseas locations.

The pattern of transaction observed in these newly opened accounts were not found consistent with the reason provided. Transactions were carried out through debit Vouchers and loose cheques and a complex layering of funds was created so that source or end use of funds cannot be traced.

While conducting EDD (Enhanced due diligence), it was found that these accounts were opened purportedly for obtaining VISA to pursue overseas studies through manpower agents/consultant agencies without supportive documents.

Funds involved in these specific complex layering transactions were suspected to be originated from manpower agents/consultant agencies. Agencies who offered assistance to students in overseas admission provided the list to open these accounts.

Moreover, Bank started to receive few e-mails from overseas universities to verify the genuineness of balance certificate that were found to be fake during the same period.

It is suspected that huge amount of dirty money was laundered through this modus operandi to obtain student VISA that may result in rise of number of illegal migrants and also aid in human trafficking in near future.

Few consultant agencies were detected in our banking channel and there is a possibility that the same modus operandi may be followed by similar entities in other banks as well which raises the magnitude on which these purported activities may be happening across the country.

Case 5

Suspected of drug trafficking through smuggled gold

DESCRIPTION: Obtaining a loan backed by contraband gold. Allegedly used to launder funds derived from drug trafficking

Steep rise in AML alerts pertaining to " transaction involving a location with high TF risk for amount of 1200 USD and above in a day" in international bordering area of country during January 2022 to August 2022.

The subject geographical area lies in the vicinity of Golden Triangle which are sensitive locations for smuggling of Gold and drug trafficking.

Sudden rise in Gold loan portfolio of the bank by more than 200% was observed in the vicinity. Transactions carried out in multiple branches of the bank at same location.

All AML alerts were having common attributes such as multiple smaller value gold loans against pledged gold availed from different branches of same bank during the same period. The value of the pledged gold articles was intentionally kept below the threshold limit to avoid the need of proof of ownership and thus multiple customers worked as a group. It was difficult to ascertain ownership as the quantity of gold pledged is of smaller value. Such suspicious pattern of transactions not observed earlier in these accounts.

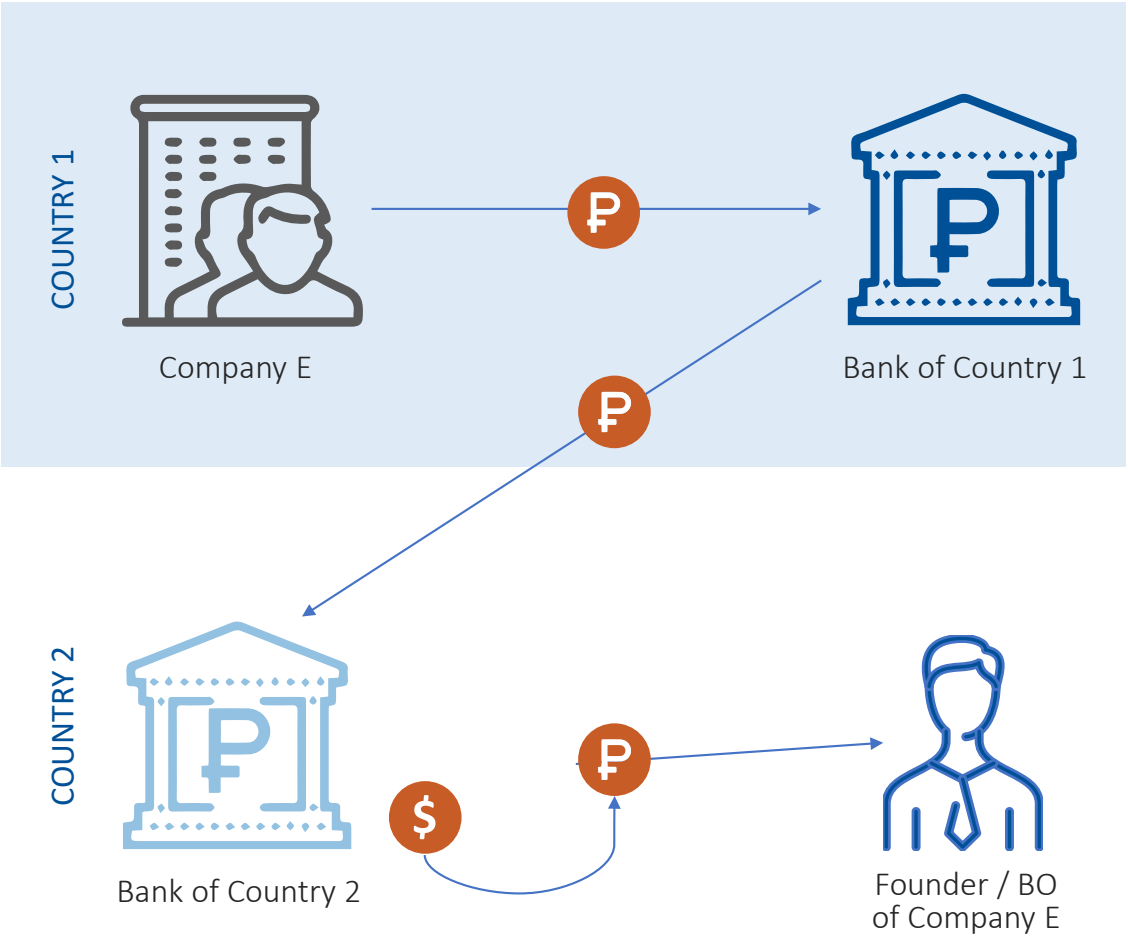
It was observed that multiple customers were approaching multiple branches in the same area to avail loans against pledged gold specifically in smaller value despite being charged processing fee every time. The disbursed funds were transferred to a few particular individual accounts, followed by immediate cash withdrawal after availing the loan from different branches. On few occasions customers prematurely closed the loan accounts to avail higher limit on the same gold articles pledged. It was suspected that the pledged gold did not belong to the pledgor and was given to them by some unknown entity/person. Therefore, the disbursed amount, withdrawn in cash was suspected to be accumulated by unknown entity/person.

During the same period, multiple news articles about seizure of smuggled gold from a neighboring country (adverse media reports) was observed. Sudden spurt in gold loan portfolio of the bank combined with adverse media report regarding smuggled gold, raised suspicion that using this modus operandi the laundered money could be used for drug trafficking/ terrorist financing as this geographical area is sensitive for such activities.

Case 6

Withdrawal of funds using fictitious international contracts

DESCRIPTION: The director of insurance company A in country 1 stole funds by deception. The funds were then transferred to the account of company "E" in country 1 as an insurance claim for damage to a ship (an oil tanker). However, company E was not in fact a client of company A and no insurance report was drawn up. Further, part of these funds were transferred to the account of company E in country 2 for laundering purposes.



CHAIN OF TRANSACTIONS

- In November, company E (Country 1) opened accounts with a Bank in Country 2.
- Through SWIFT, two transfers from the company's account opened with a bank in Country 1 were made to the bank in Country 2 on the basis of "transfer of own funds".
- The funds were then converted into foreign currency on the same days and then part of the funds were withdrawn in cash by cheque through the founder/beneficial owner of the company.
- A couple of days later, additional funds were received in a similar way from Country 1 on the basis of "transfer of own funds".

SUSPICION CRITERIA

The bank in Country 2 requested information on the activities and source of funds of the client.

The client provided a Memorandum of Agreement according to which Company E sold the ship to company “Africa” (Country 1)

Also provided an Investment Agreement stating that Company E is financing “Antarctica” Ltd (Country 2) to explore and develop a gold deposit.

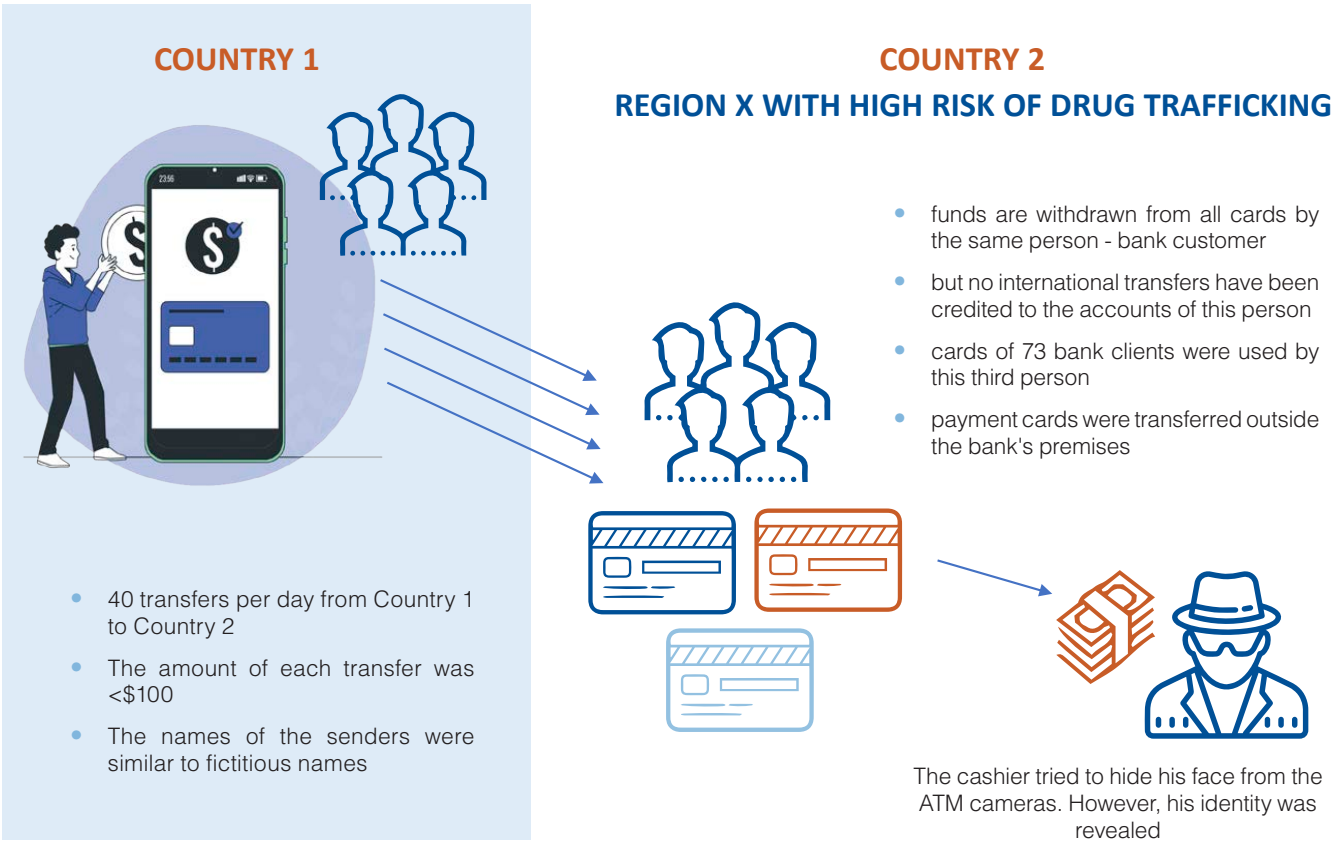
An analysis of the activities, documents and transactions provided showed the following indications of suspicion:

- Transactions unrelated to the client's core business.
- Transfers of own funds from one bank to another for no apparent reason, including international transfers.
- Large transfers, conversions and cash withdrawals.

Case 7

Cashing of funds derived from drug trafficking

DESCRIPTION: A large number of transfers to Country 2 customers' accounts were detected, but the amounts were not significant. Receipts were made through self-service terminals (Visa Direct) located on the territory of Country 1, which allowed the transfer of small amounts without identifying the customer. All the funds that were deposited into the accounts were withdrawn from ATMs via bank payment cards. As a result, these cards were known to be withdrawn by the same person, although the person was not the cardholder.



The monitoring of customer transactions revealed a large number of transfers to customer cards. The amount of transfers was insignificant and in most cases was less than $100. Customer accounts received up to 40 such transfers per day. All accounts were attached to payment cards that had been issued from a bank branch in an area with a high risk of drug trafficking. Funds were received from Country1 self-service terminals and the names of the senders were similar to fictitious ones.

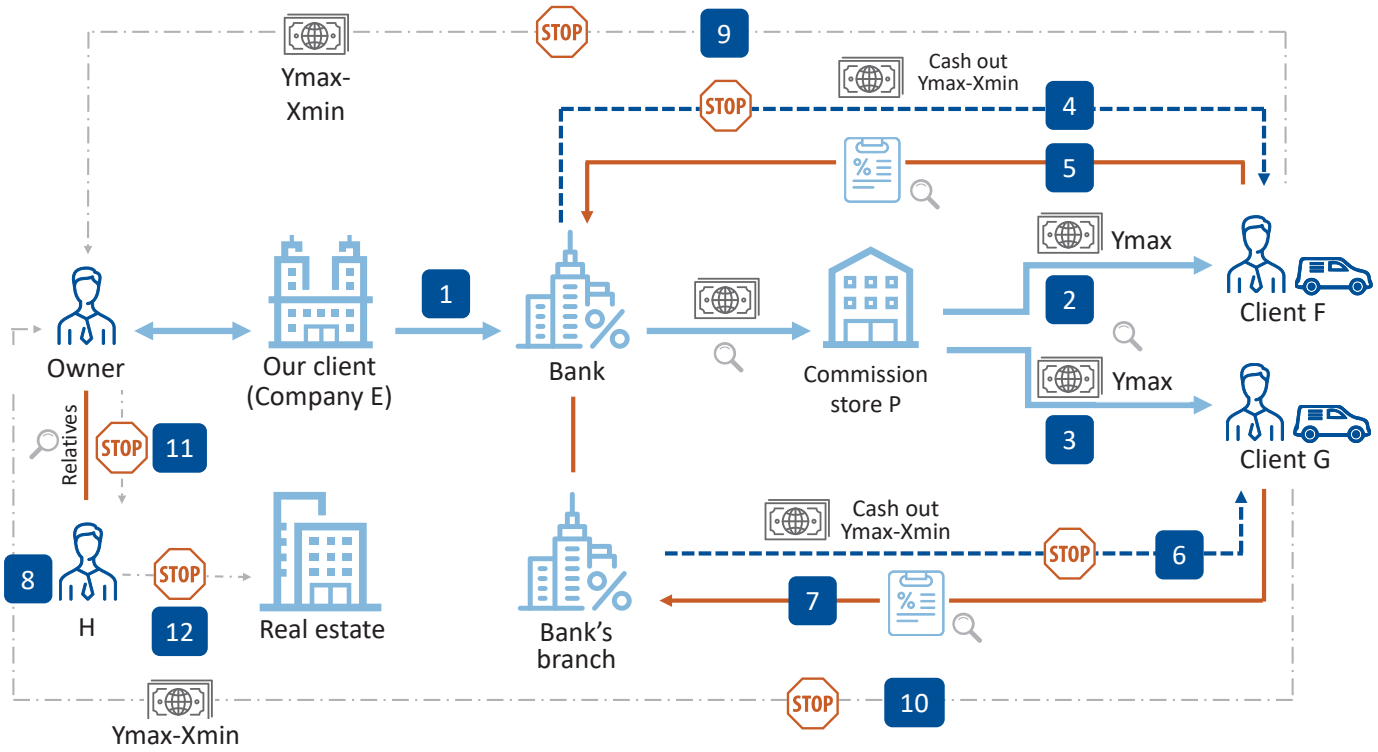
The analysis of customer transactions revealed that the funds were withdrawn from the cards of 73 customers by the same person. His identity was established through video camera recordings. The analysis of this customer's accounts revealed no correlation with the originators and beneficiaries of the analyzed transfers. The monitoring results were sent by STRs to the AML/CFT designated authority of the country. Further joint work was carried out with the authorised body, additional and updated information was provided regarding the customers and their accounts. The cards were not blocked to identify all interrelationships.

After two months, the media reported the arrest of a group of drug traffickers in Country 1. Among the detainees was a bank customer who was withdrawing funds from 73 bank customers. It turned out that the proceeds were funds from drug trafficking. The group issued payment cards in the names of compatriots and then conducted transactions on their cards themselves, the cards being transferred outside the bank premises.

Case 8

Attempting to cash out fraudulently on an organisational basis

DESCRIPTION: Company E, in order to cash out a certain portion of the income received in a bank account in non-cash form, plans to purchase goods under a fictitious scheme. As a result, company E decided to purchase cars in the company's name from citizens F and G. For this trading operation, company E used the services of a commission store P. The purchase by company E of cars from two different owners (F and G) through the same commission store and the transfer of cashless funds to the bank cards of the vendors on the same day for both cars, raised some suspicion about the validity of the present transaction.



In accordance with the legislation of Country A, legal entities and entrepreneurs must carry out their business activities in non-cash form through a bank account. Cash turnover is strictly regulated under the law. There are strict limits on withdrawals from the bank account.

To circumvent these restrictions, i.e. in order to cash out a certain portion of the non-cash income received in the bank account, Company E plans to purchase goods under a fictitious scheme. As a result, company E decided to purchase cars in the company's name from citizens F and G. For this trading operation, devised to cash out non-cash, company E used the services of a commission store P.

The purchase of cars by company E from two different owners (F and G) through the same commission store and the transfer of cashless funds to the bank cards of the vendors on the same day for both cars, raised some suspicion about the validity of the present transaction.

For this reason, analysis was initiated into the market prices of the cars being purchased through various sources. As a result of examining the information received from several sources, it was found that, based on the condition of the vehicles, their average market value was in the range Xmin~Ymax. It was found that the value of both the vehicles purchased by Company E is within the average market price range. But we should note that the value of the cars is very close to the Ymax price.

The monitoring activities continued even after company E had made payments to citizens F and G. That is, there was constant monitoring of what purposes the funds of citizens F, G were used for when they sold the cars, and each payment made with a bank card was analysed separately.

After a few days, customer F came in to withdraw large amounts of cash from his bank card. He was asked why he wanted to withdraw large amounts of cash immediately, the client replied that he had purchased a property and needed to pay for it. For the reason that it was possible to pay for it with a bank card, the bank told the customer that it would collect the cash soon and additionally asked him to bring the contract for the purchase of the real estate.

The next day at the bank branch the exact same incident was repeated with customer G. He gave the same answer as customer F and the bank replied that he will raise the requested amount of cash and the customer will be notified as soon as possible and he was asked to bring the real-estate contract. Thus, the real estate contracts received from clients G and F were analysed as soon as possible.

BASED ON THE INFORMATION RECEIVED FROM THE PARTIES, THE FOLLOWING CIRCUMSTANCES WERE ASCERTAINED:

Submission by both clients G and F to the parent bank and the branch office of the same contract for the purchase of the real estate as the basis;
The naming of a third customer H as the purchaser of the real estate in the contract;

Matching the name of customer H with the name of the owner of company E, the patronymic of customer H with the name of company E. On further analysis of this, it transpired that client H is the son of the owner of company E;

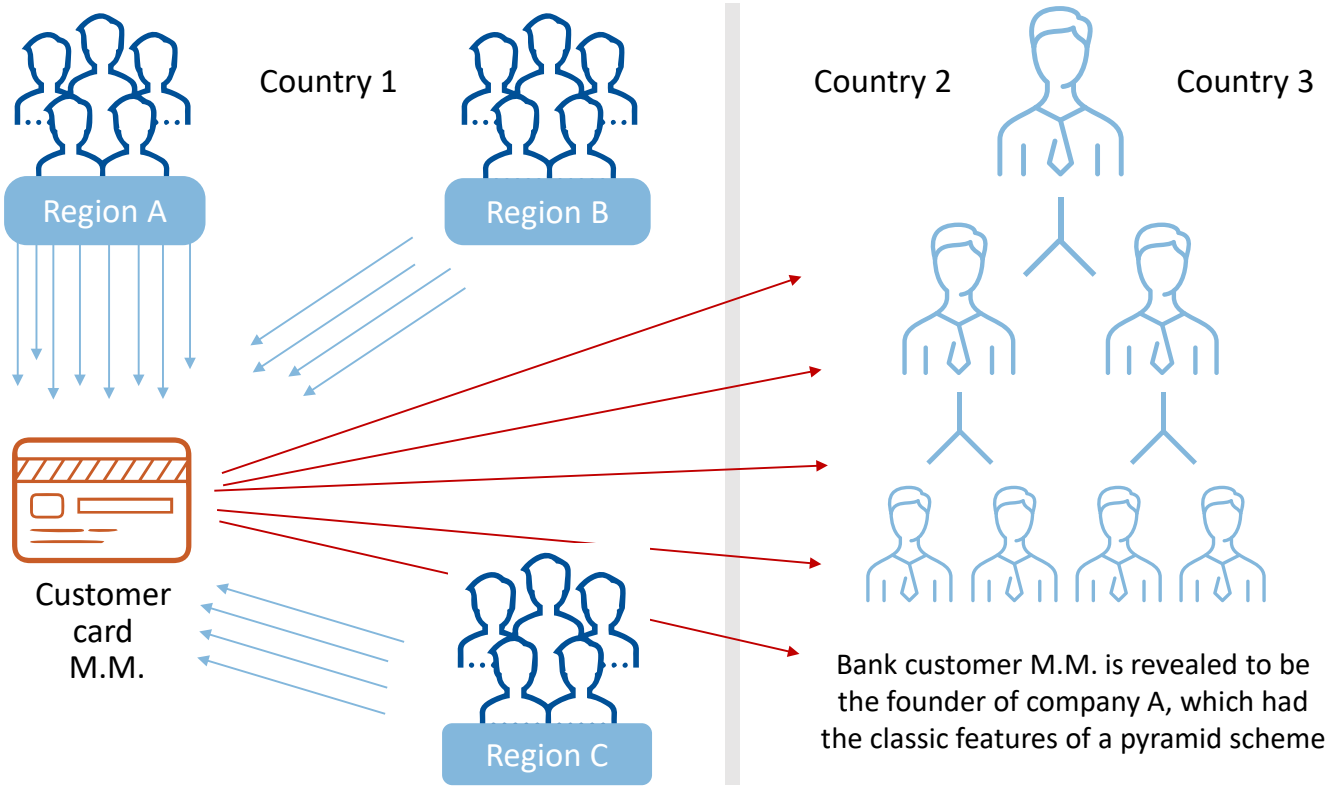
Company E actually purchased the cars from the owners (G and F) slightly cheaper than the X_{min} price. However, Company E has bought the cars from G and F at a price close to Y_{max}, with the condition that it would return the difference in cash (Y_{max}- X_{min} = price difference) to itself;

In the end, the main goal of company E is to cash out the legal non-cash money from the bank account in the necessary amount in order to purchase real estate for his son (H).

Case 9

Identifying pyramid schemes

DESCRIPTION: M.M., an individual client of the Bank, received funds from third parties from different regions to his plastic card account. The incoming funds were then sent by money transfer to foreign countries (including the FATF grey list countries). This fact aroused the bank's suspicion. In addition, an analysis of the internet revealed an advertisement for company A, the founder of which was Bank customer M.M. The advertisement contained signs of a pyramid scheme.



The front office serving the bank's customers discovered that card deposits were being made from other individuals, with customers talking about interest and profits of some kind. At the same time, the internal control officers of the regional smart banks reported that unknown cards issued by client "A" Ltd .were being sold.

Compliance control analysis revealed that the plastic card was mainly used by an individual who was the director, and he was also the founder of client “A” Ltd, a firm that was serviced at one of the bank's branches.

Analysis of his activities as the director of "client A" showed that he received transfers "from an individual to an individual" from different cards, which were deposited in cash and non-cash form from different regions of the country 1. At the same time, the director is a citizen of country 2 who is a non-resident of country 1 holding the passport of country 2.

Despite the fact that Client A Ltd. was not engaged in any active activities and accordingly did not conduct transactions specifically as a legal entity, it nevertheless opened secondary accounts in other branches of the region and in smart banks.

All funds were not transferred to the legal entity, but to its individual director. The incoming funds were then sent by money transfer to country 2 and country 3, which is on the FATF grey list.

Analysis of internet resources (social media) showed that Client A Ltd. distributes advertisements offering to buy gold jewellery within a certain time frame with a high profit margin.

Thus, it turned out that Client A Ltd. was created as a shell for a pyramid scheme and all the criminal proceeds were deposited into the accounts of its director.

All transactions of the individual client were blocked and the activities of the legal entity client were suspended. The relevant STRs were sent to the FIU.

EAG

2022