ASIA ALLIANCE BANK

Money Laundering and Sanctions Program:

Transaction Monitoring and Reporting Procedure

Tashkent – 2024

Abbreviations:	
Bank	"ASIA ALLIANCE BANK" AJ
Anti-money laundering	Fight against money laundering
TM	Financing of terrorism
FPWMD	Financing the proliferation of weapons of mass destruction
STR	Notification on a suspicious transaction
SAR	Notification on a suspicious case
The Central Bank	The Central bank of the Republic of Uzbekistan
BBA	Base Billing Amount
IR	Information request
TMT	Transactions Monitoring System
KYC	Know Your Customer
QC	Quality control
Alert	Doubtful case
Case	Suspecious case
IRN	Internal Referral Notification
List	The list of information provided by state bodies and other competent bodies of the Republic of Uzbekistan, which fight against terrorism and proliferation of weapons of mass destruction , as well as, persons participating or suspected of participating in terrorist activities or distribution of weapons of mass destruction organized by a specially authorized state body on the basis of information provided through official channels from the competent authorities of foreign countries and international organizations
Scope of activity	Employees responsible for customer service and customer banking operations, including managers
Internal and external legal documents :	
The law of the Republic of Uzbekistan "regarding Banks and banking activities";	
The law of the Republic of Uzbekistan No 660-II dated August 26, 2004 of the Republic of Uzbekistan "on combating money laundering, terrorist financing, and the financing of proliferation of weapons of mass destruction";	
"Internal Control Regulations for combating money laundering, terrorist financing, and proliferation financing of weapons of mass destruction in commercial banks" registered under No 2886 dated May 23, 2017 at the Ministry of Justice of the Republic of Uzbekistan.	
The Regulation "regarding suspension of operations of persons included in the list of persons participating or suspected of participation in terrorist activities or distribution of weapons of mass destruction, suspension without use of funds or other property, on the procedure for allowing the use of suspended property and resuming operations" registered under No 2237 dated October 19, 2021 at the Ministry of Justice of the Republic of Uzbekistan.	

Regulation "On the procedure for monitoring the validity of foreign currency transactions by legal entities and individuals" registered under No 2467 dated June 12, 2013 at the Ministry of Justice of the Republic of Uzbekistan;
Regulation "Suspension of operations of persons included in the list of persons participating or suspected of participation in terrorist activities or distribution of weapons of mass destruction, suspension without use of funds or other property, on the procedure for allowing the use of suspended property and resuming operations" registered under No 3327 dated October 19, 2021 at the Ministry of Justice of the Republic of Uzbekistan.

1. General provisions

This procedure is designed to determine and prevent the recorded cases for combating money laundering, terrorist financing, and the financing of proliferation of weapons of mass destruction taken from the activity of "ASIA ALLIANCE BANK" JSC (hereinafter referred in as the Bank). To this end, the Bank undertakes the responsibility of following the regulations and legislation connected with complying with all applicable Anti-Money Laundering and Sanctions laws and regulations, including Suspicious Transaction/Activity Monitoring, Suspicious Transaction Monitoring and Suspicious Transaction/Activity Reporting.

1.1. Scope of application

This Procedure "Transaction monitoring and reporting" *(hereinafter referred in as the Procedure)* belongs to all customers, leaders, employees, lines of activity and other structural divisions, It is intended to regulate the daily activity of bank employees, which includes transaction monitoring and reporting.

1.2. Related internal regulatory documents

This Regulation should be read together with the following internal regulatory documents:

- ✓ The Bank's Anti-Money Laundering, Terrorist Financing and FPWMD and Sanctions Policy;
- ✓ Regulation of the Bank's Compliance Control Department.
- ✓ Bank's Know Your Customer (KYC) Procedure;
- ✓ Bank's Sanctions Check (SS) Procedure; and
- ✓ Bank's Risk Assessment (RA) Procedure.

2. Purpose

This Regulation serves as a guide for compliance with the rules of combating money laundering, monitoring of transactions, and compliance with the requirements for preparing reports on suspicious transactions.

The purpose of this Procedure is to facilitate proper monitoring of transactions conducted or attempted to be conducted by or through the Bank. Identifying and reporting suspicious activity is an important component of the Bank's Anti-Money Laundering and Sanctions Compliance Program.

This Regulation is intended to assist the Compliance Control Department in meeting the Bank's expectations regarding the processes, activities and controls established as part of the anti-money laundering and sanctions control environment.

Areas of activity and the Compliance Control Department shall have the following minimum objectives in implementing this Procedure:

- The process of reviewing a "suspicious case" (Alert) created through transactions monitoring system or by the employees of the field of activity shall be prevail and this "Suspicious case" (Alert) shall be implemented in chronological order, through analysis of operations performed during the past period;
- Monitoring of "Suspicious case" (Alert) and their control ensures individual compliance with their deadlines and execution in the appropriate time interval;
- The script of "Suspicious case" (Alert) and transactions details shall be conducted in order to determine the existence of grounds for preliminary review process for unusual additional checks applicable to objectively assess and effectively dispose of these cases;

- The client and any related parties are subject to a wide range and comprehensive investigation for "Suspicious case" (Alert) requesting the additional inspection;
- The documents related to the "Suspicious case" (Alert) should be documented in electronic form;
- If a suspicious transaction is detected, if there are relevant indicators, the Compliance Officer may conduct a comprehensive analysis and classify the transaction as suspicious;
- If suspicious activity is confirmed, the respective actions should be taken (for example, preparing the reports of STR or SAR and submit them to the special authorized bodies of the Republic of Uzbekistan);
- Ensure all internal records retention policies comply with applicable regulatory requirements.

3. Liability and Responsibility

This paragraph determines the liabilities and responsibilities of the employees in terms of "*Transaction Monitoring and Reporting Procedure"*.

3.1. Employees of the field of activity

The employees of the field of activity assume the following responsibilities and responsibilities:

- Determination of unusual customer behavior, "Suspicious case" (Alert) or activity in the bank account and send the form of internal forwarding message to the head of activity.

3.2. Head of activity

The head of the field of activity assumes the following responsibilities and responsibilities:

- Review the internal referral message form documented by the staff of the activity line and submit it to the employee of the Compliance Control Department;
- Review and respond in detail to Internal Referral messages submitted by line of business staff;
- Taking steps to terminate business relationships with a client due to suspicious activity or increased risk identified in consultation with the Compliance Office.

3.3. Employees of the Compliance Control Department

Employees of the Compliance Control Department assume the following responsibilities and responsibilities:

- Carry out a "Suspecious Case" investigation and submit this "Suspecious Case" to the Deputy Head of the Compliance Control Department for further review;
- Investigate non-problematic "Doubtful case" (Alerts) and make recommendations as to whether or not they should be escalated;
- Determining unusual operations and escalating them as "Doubtful case" (Alert) for consideration by the Deputy Head of the Compliance Control Department;
- Second review of the Internal Referral Messages form provided by the head of the department or activity areas;
- Filling up the form of submission of the project of notification of preliminary STR or SAR.

3.4. Deputy Head of the Compliance Control Department

The Deputy Head of the Compliance Control Department assumes the following responsibilities and liabilities:

- Conduct a “Suspecious Case” (Case) study and recommend that the case be reviewed by the head of the Compliance Control Department;
- Review of “Doubtful Case” (Alert) and "Suspicious case" (Case) escalated by the staff of the activity line and the staff of the Compliance control department;
- Filling up the form of submission of the project of notification of preliminary STR or SAR;
- Analyze to add, modify and delete rule scripts and upload them to Transaction Monitoring System or upload them to a file;
- Set limits and analyze settings and upload them to Transaction Monitoring System;
- Carrying out the duties of the head of the compliance control department in case of his temporary absence due to certain reasons;
- Reviewing internal referral messages and receiving information from employees of the relevant line of activity;
- Reviewing the report of sending notification of STR or SAR;
- Supervise staff involved in transaction monitoring and reporting;
- Oversee reporting of information related to requests from relevant regulatory authorities;
- • Monitoring the timely implementation of investigations of "Doubtful cases" (Alert) and "Suspicious cases" (Case).

3.5. Head of the Compliance Control Department

The head of the compliance control department assumes the following responsibilities and responsibilities:

- Monitoring the effective functioning of the main components of the compliance control department;
- Review reports on escalated and potential issues, issues, and transaction monitoring activities;
- Final review of the report on STR or SAR;
- Conduct quality control audits on work arrangements;
- Finalize what should be added, changed and deleted from the rules script;
- Revision and final approval of limit setting;
- Approving special reviews and updates to relevant internal regulatory documentation;
- Regularly inform the Management about the recognition of the client's operation as a suspicious operation;
- Reporting on STR or SAR to Department for Combating Economic Crimes at the General Prosecutor Office of the Republic of Uzbekistan.

3.6. Deputy chairman of the Board

The deputy chairman of the board assumes the following responsibilities and responsibilities:

- • Approving the termination of a business relationship with a client due to suspicious activity or high risk identified in consultation with the head of the Compliance Control Department and the head of the ROBS (Practical Department).

3.7. Chairman of the Board

The chairman of the board assumes the following responsibilities and liabilities:

- Consult with the head of the Compliance Control Department and the head of the relevant department and the head of the ROBS
- (Operational Department) on making a decision on the issue of continuing relations with a client whose level of risk has been proven to be dangerous;
- If necessary, escalation to the Bank Council in order to prevent relevant risks and problems and make relevant decisions.

3.8. Responsibilities and liabilities of the employees of the bank

The Bank, including the employees of the Compliance Control Department, managers and employees of other departments shall be liable in accordance with the law for violation of this Order.

The Bank shall ensure that its payment agents and sub-agents comply with the requirements of this Regulation.

The Bank is responsible for the violation of the requirements of this Regulation by its payment agents and payment sub-agents.

Legal documents, as well as legal documents in the field of combating the legalization of proceeds from criminal activities, financing the development of terrorism and the spread of mass destruction, in the event that the bank employees committed violations in the course of transactions, the bank employees shall immediately deliver these evidences in writing to the head or employees of the Compliance Control Department.

4. Real time monitoring

Employees of the Compliance Control Department use the transaction monitoring system to perform real-time monitoring of the customers identified with the following high-risk category, as noted in paragraph 10.3 of the "Know Your Customer" (KYC) procedure:

a) Listed persons or organizations owned or controlled by a Listed person, direct or indirect owners or controlling persons of the Listed organization;

b) persons permanently residing, staying or registered in countries that are considered to have strategic deficiencies in the field of combating money laundering and terrorist financing;

d) persons permanently living, residing or registered in the offshore territory;

g) organizations whose beneficial owners are the persons specified in subparagraphs "a)" and "b)" of this paragraph;

j) high-ranking officials (PEP), their close relatives and persons close to high-ranking officials;

m) organizations whose beneficial owners are the persons specified in subparagraph "d)" of this clause;

o) entrepreneurs dealing with jewelry, precious metals, works of art and antiques;

s) s) organizations whose beneficiary owners are the persons specified in subsection "j)" of this clause.

Continuing the transactions

According to these transactions, the operation is carried out if it indicates **the usual activity characteristics** that do not create a "suspicious case" and if the activity determines the existence of **a legal basis or business purposes**.

Liquidation of the transactions

If an employee of the Compliance Control Department suspects that this transaction is unusual or related to the legalization of proceeds from criminal activity, they must take the following enhanced measures:

- collecting and recording additional verified information about the client from open sources and databases;
- receive information from the client about the funds or sources of wealth for the operations carried out by him;
- study the objectives of operations planned or carried out by this client;
- continuously monitor operations performed by the client.

Strengthened customer due diligence measures, namely, obtaining information from the customer about the sources of funds or other assets for the operations carried out by him and (or) planned or carried out by this customer if it is **not possible** to study the purposes of the operations, the Bank will refuse to carry out the operations of such a client and will study the measures to terminate practical business relations with the client.

5. Monitoring over the suspected activity

5.1. General provisions rlated to the suspected activity

This policy defines the procedure for full, accurate and timely identification, investigation and reporting of potentially suspicious activity in the Bank.

All employees of the bank are responsible for the prevention, detection and reporting of money laundering through escalation any activity or information to the head of the activity and the Compliance Control Department related to combating money laundering, financing of terrorism, financing of weapons of mass destruction or related to financial crimes. Therefore, all employees of the Bank must be vigilant and aware of unusual activities or red flags in the fight against money laundering, proliferation of weapons of mass destruction and financing of terrorism in the course of their work.

Suspicious activity can be detected in several ways. This includes the concealment or concealment of funds derived from illegal activities and the concealment or concealment of funds or assets related to illegal activities.

Suspicious activity - should include the regulatory criteria established on the basis of the legal procedure and the series of **suspicious transactions** determined on the basis of the Bank's risk approach. Suspicious transaction - prior to making a decision to include (not include) this transaction in the category of suspicious transaction, there are reasonable suspicions that this transaction was carried out by the Bank for the purpose of legalization of proceeds from criminal activities, financing of terrorism and (or) financing of distribution of weapons of mass destruction. is an existing practice.

*According to the **paragraph 48** of the Regulation registered under No 2886* if one of the following criteria and symptoms is present, this operation is defined as "suspicious":

1. an operation or a customer performing it, which has been assigned a high level of risk by a commercial bank;
2. regular return of the amount previously received by the resident-customer to the benefit of the non-resident under the goods delivery (performance of work, service) contract;
3. suspicion of the authenticity (reliability) of the documents submitted for the operation and (or) the fact that the information about the operation, including about one of the parties performing the operation, does not correspond to the information available in the commercial bank;
4. abnormal behavior of the client when applying for the operation (assignment, petition), for example: nervousness, hesitancy, his aggressiveness in the presence of persons controlling the client's actions, or his contacting other persons for advice over the phone for trivial reasons;

5. the customer's unusual concern about confidentiality issues or the customer's unjustified refusal or unreasonable delay in providing the information requested by the commercial bank about the operation;

6. it is not possible to identify the client's partners for the operation being carried out;

7. the operation does not have a clear economic nature and does not correspond to the description and type of activity of the client;

8. regardless of the description of the client's activity and (or) the activity of the client's account is low for a period of more than three months or the activity stops, and then there is an unreasonable increase in the circulation of funds in his account 'increase;

9. Unreasonable and (or) premature termination of business relations by withdrawing all funds or transferring them to other commercial banks at the initiative of the client;

10. immediate termination of business relations at the initiative of the client when the measures specified in these Rules are reasonably applied by the commercial bank to the client;

11. clear inconsistency of operations performed by the client with the participation of a commercial bank to the generally accepted practice of conducting operations;

12. Unreasonable distribution of sums of operations similar to the operations performed by the customer in a total amount equal to or exceeding 500 times the basic calculation mechanism set on the day of the operation;

13. the settlement procedure consists of non-standard or unusually complex schemes that differ from the customer's usual activity;

14. exchange of banknotes of one value for banknotes of another value by an individual in an amount equal to or exceeding 500 times the base calculation mechanism established on the day of exchange;

15. an individual transfers funds in the form of cash to the bank account of a legal entity or an individual entrepreneur in an amount equal to or greater than 500 times the base calculation mechanism established on the day of the operation, to the loan, financial assistance, chartered fund (capital) to be entered as an investment or replenishment of working capital;

16. transfer of funds from the accounts of legal entities or individual entrepreneurs in the amount equal to or greater than 1000 times the base calculation mechanism established on the day of the transaction as financial assistance or debt;

17. transfer of funds from the accounts of legal entities or individual entrepreneurs to the benefit of individuals in an amount equal to or greater than 1000 times the basic calculation mechanism established on the day of the transaction as a dividend or income;

18. cash withdrawal from the account of an individual in the amount equal to or greater than 500 times the base calculation mechanism set on the day of the transaction;

19. execution of operations (payment or cash withdrawal) from one counterparty's terminal during one day from five or more international payment cards in the amount equal to or exceeding 25 times of the operation of each card of the base calculation mechanism;

20. transfer of funds outside the territory of the Republic of Uzbekistan to the account of the recipient opened in a bank located in a different region from the place of registration of the recipient in an amount equal to or greater than 500 times the basic calculation mechanism established on the day of the operation.

According to the risk approach of the bank if one of the following criteria and symptoms is present, this operation is also defined as "suspicious".

1. Using the client's bank cards, through the mobile applications of other banks and payment organizations, simultaneously or multiple times for a period not exceeding 30 days, to one or more bank cards in a total amount equal to or exceeding 500 times the base calculation mechanism or transfer to electronic wallets;

2. Implementation of "P2P" transfers of funds to one individual or several individuals with several transactions in one day or several days, in an amount that does not correspond to the usual turnover of the client's Bank cards 3 times;

3. Regular receipt of funds from other plastic cards in the total amount equal to or greater than 250 times the base calculation mechanism through "P2P" transfers to the client's bank cards and converted on the same day;

4. Monitoring with particular attention to funds in P2P transactions (in the unit whose last digits are not equal to zero) carried out using the client's bank card account numbers.

5.2. Types of suspicious activity monitoring

5.2.1. Manual monitoring of the suspicious monitoring

Employees of the Bank's Activity Department identify "Suspicious Situations" of the client and immediately report such transactions to the Head of the Activity Department and the employees of the Compliance Control Department in writing.

Each employee of the Activity Department shall follow the following procedure in case of detection of unusual activity of the client:

- Assessing the formation of a red flag based on an unusual condition detected in the client's activity or behavior;
- Review of customer “KYC” file;
- View customer transaction history;
- Determining whether unusual activity is unusual for the account;
- Preparation of internal referral message:
  - Describes the event that happened;
  - Provides a list of specific transactions and supporting documents, if any;
  - Lists the grounds for determining that an activity is potentially unusual.
- Escalation of the internal referral message to the head of the activity line.

(The internal referral message form is given in Annex A)

The employee of the Compliance Control Department enters the Internal Referral message about "Suspicious Situation" into the Special Journal. A special log is maintained electronically in the Transaction Monitoring System or in an electronic file. Also, depending on the type of escalation, the employee of the Compliance Control Department is responsible for correctly entering the information in the Internal Referral message into the Special Journal (the form of the Special Journal is provided in Appendix B).

Line of Operations personnel should not attempt to conduct their own investigation prior to escalating a Suspicious Case Internal Referral. At the same time, Operations personnel must ensure that files are maintained that show the identity of the client in question, the type of activity, and why the transaction is considered unusual or suspicious.

5.2.2. Automatic monitoring of suspicious activity

The bank uses a transaction monitoring system with rule-based automated management, designed to identify transactions that meet a predetermined risk level and to identify cases that fall under the established criteria for a suspicious and (or) suspicious transaction. Officers responsible for investigating Suspicious Cases generated through this system should review existing KYC data and other relevant information to determine whether the activity is considered potentially unusual.

5.3. Procedure for consideration of "suspicious cases".

5.3.1. 5.3.1. Review of "suspicious cases"

The employees of the activity department carry out the process of submitting an Internal Referral message on "Suspicious Case" based on the following steps:

- Escalation type (manual or automatic);
- Case type (typology of fight against money laundering, Red flags or negative news);
- Previously escalated STR or SAR;
- Comments reflected in the internal referral message.

As part of the Suspicious Case initial review process and depending on the type of transaction being investigated, Operations staff will either automatically enter the relevant information into the Bank's system or electronically log it when they wish to escalate manually. *(The journal in electronic form is presented in Appendix C)*

5.3.2. Review of transactions

A comprehensive review

After the detection of a "suspicious case", the employees of the Activity Department must review all the operations carried out within one month. If necessary, the staff of the Operations Department may extend the period of review of transactions for the current account or to a certain extent to review the activity of the customer.

Analyze the red flags

Unusual customer behavior or activity in a transaction is often referred to as a red flag. Also, analyzing red flags can indicate money laundering, terrorist financing, and proliferation of weapons of mass destruction. A “Suspicious Case” generated by manual or automated functions means one or more red flags indicating potentially unusual activity. As part of the 'suspicious case' review process, Operations personnel are required to review internal and external customer transactional activity in the context of the red flag(s) that gave rise to them. However, it should be noted that the presence of a red flag does not in itself constitute evidence of money laundering, proliferation of weapons of mass destruction, or financing of terrorism.

5.3.3. Investigation of "suspicious cases".

Reviewing the previous STR or SAR files

The staff of the activity line will check whether there is a message about the client through the internal database of the Bank, whether there is a notification about the STR or SAR against the client. If there is a message about the client's STR or SAR before, the staff of the activity line will mark "Previously available" in the internal referral message. Also, this Internal referral message should include the number, date and all details of the previous STR or SAR.

Review of customer KYC file

The line officer will review the customer's KYC form. It will review the customer's previous "suspicious transactions" information in the KYC form, if any. During the KYC verification, the line officer should record any information that could mitigate or increase the risk identified in the "Suspicious Case" in the appropriate Internal Referral Message.

The employee of the Compliance control department performs the following actions according to the internal referral message sent by the employee of the activity department:

- studies information;
- enters relevant information into the terrorist financing system inspection log or the Special electronic log;
- registers the client in the KYC form;
- escalates to the head of the Compliance Control Department, when there are sufficient grounds, to classify the transaction as suspicious or suspicious;

Review of the activity of the customer

In order to adequately investigate "suspicious situations", the employee of the Compliance Control Department checks whether the operations performed by him do not correspond to his activities recorded in the KYC form.

Searching in negative news

The process of searching for negative news should be carried out in relation to enterprises that have implemented "suspicious situations" and their counterparties. Using the public domain to search for negative news, the line of business staff will search with the following search strings:

- **"Mijoz nomi" and** “abuse” or “allegation” or “arrest” or “blackmail” or “breach” or “bribery” or “convicted” or “corruption” or “criminal” or “drug” or “embezzle” or “evasion” or “extremist” or “fined” or “forge” or “fraud” or “guilty” or “illegal” or “money laundering” or “politically exposed” or “prison” or “prosecution” or “sanctions” or “scam” or “scandal” or “stolen” or “suspect” or “terrorist” or “theft” or “trafficking”.
- **"Мижоз номи" и** “злоупотребление” или “обвинение” или “арест” или “шантаж” или “нарушение” или “взяточничество” или “осужденный” или “коррупция” или “преступник” или “наркотические вещества” или “хищение” или “уклонение” или “экстремист” или “оштрафованный” или “подделка” или “экономическое преступление” или “виновный” или “незаконный” или “отмывание денег” или “политически значимый” или “тюрьма” или “обвинение” или “санкция” или “мошенничество” или “скандал” или “украденный” или “подозреваемый” или “террорист” или “кража” или “незаконная торговля”.
- **"Mijoz nomi" va** “suiste’mol qilish” yoki “da’vo” yoki “hibsga olish” yoki “shantaj” yoki “buzish” yoki “poraxo‘rlik” yoki “mahkum” yoki “korrupsiya” yoki “jinoyat” yoki “narkotik moddalar” yoki “o‘zlashtirish” yoki “qochish” yoki “ekstremist” yoki “jarimaga tortilgan” yoki “soxta” yoki “iqtisodiy jinoyat” yoki “aybdor” yoki “noqonuniy” yoki “daromadlarni legallashtirish” yoki “yuqori mansabdor shaxs” yoki “qamoq” yoki “ayblov” yoki “sanksiya” yoki “firibgarlik” yoki “janjal” yoki “o‘g‘irlangan” yoki “gumon qilingan” yoki “terrorchi” yoki “o‘g‘irlik” yoki “savdo/noqonuniy ayrboshlash”

The practice staff will determine whether additional searches are necessary, including searches for alternative name changes. If the employees of the field of activity cannot clarify this issue, they should contact the employees of the Compliance Control Department, who, in turn, will review it based on their professional qualifications.

It should be noted that all identified negative news is not considered relevant in the process of continuing business relations with the client. Negative news is divided into "relevant" and "non-relevant" types.

Below are some examples of "relevant" and "non-relevant" types:

Respetive negative news

- Terrorist activities related to the financing of terrorism and the financing of weapons of mass destruction;
- Legalization of proceeds from criminal activities and non-compliance with Sanctions;
- Crimes related to drugs;
- Fraud related to the legalization of proceeds from criminal activities;
- Bribery related to money laundering;
- Persons on blacklists or watchlists as determined by the government due to increased risk of money laundering;
- Decisions of law enforcement investigations (for example, indictment, arrest, etc.);
- Criminal charges or convictions (eg, indictment, arrest, etc.);
- Significant civil damages or fines due to increased risk of money laundering;
- Penalties related to the legalization of proceeds from criminal activities;
- Corrupt activity;

- the presence of the risk of legalization of proceeds from criminal activities in defamatory articles.

Non relative negative news

- criminal convictions or convictions;
- specified civil fines;
- wrong actions of employees;
- actions of former members of senior management;
- occurrence of small disputes with third parties;
- small deficiencies in the practice of activity;
- network defaults;
- A client appointed to a high political position;
- personal matters unrelated to the activities of the client or related parties.

In the case of "relevant" or "not relevant" cases in the above example category, if the staff of the activity area does not have a reasonable belief, they will consult with the employee of the Compliance Control Department.

Also, in the process of searching for negative news, employees of the activity line should check whether all available information is compatible or not based on the following standards:

- Age or year of birth;
- Geographical location;
- Name;
- Occupation or position.

5.3.4. Terminating the "Suspecious case"

After performing the following steps to check for "suspicious case", inclufing reviewing them, checking the previous STR or SAR file, reviewing KYC files, re-verifying customer activity, Employees of the field of activity shall terminate after performing information request (MS) and negative message searches. After performing the actions related to the review procedure mentioned in Section 4.3 of this Procedure, The employees of the activity area form the Internal Referral Message based on their point of view, the employee of the Compliance Control Department evaluates this Internal referral message as non-problematic and makes recommendations regarding the need to stop it or evaluate it as problematic and escalate it for further investigation.

In all cases, Operations personnel must balance the basis for handling the Internal Referral message with the Bank's knowledge of the customer and any information gathered through research. This allows the Operations staff to fully assess the risk associated with the "Doubtful Case" and take appropriate action. Employees of the line of activity must also ensure that all relevant supporting documents are stored and uploaded to the transaction monitoring system or submitted separately.

Terminating Internal Referral message

If the Compliance Officer concludes that the transaction(s) that gave rise to the "Doubtful case" does not indicate unusual activity and determines that the activity has a legitimate basis or business purpose, the employee of the field of activity makes a recommendation on finding the "Doubtful case" to be considered non-problematic and enters it into the **special log**. Special log includes:

- ordinal number;
- date of operation;

- name of the client;
- unique customer number;
- correspondent's name and country;
- correspondent bank (with MFO or SWIFT);
- type of payment (incoming, outgoing);
- transaction amount and currency;
- content of operation;
- notification date;
- name of the responsible employee who reported.
- criterion of operation (suspicious or doubtful);
- negative news check results;
- the nature of the operation (business purpose or there are suspicions of combating the legalization of proceeds from criminal activities);
- a conclusion that the operation is unusual or usual;
- work performed on the operation (termination or escalation);
- date sent to the main bank or Department for Combating Economic Crimes under the General Prosecutor's Office of the Republic of Uzbekistan.

After the employees of the Compliance Control department shall find the the Internal Referral message is not related to laundering of proceeds of crime, financing of terrorism or proliferation of weapons of mass destruction, its verification suspends the status in the Transaction Funding System or marks "status suspended" in the Special Log.

Escalation of "Doubtful case" at the level of "Suspecious case"

If the employee of the activity line concludes that the "Doubtful Case" situation is potentially unusual or high risk, in that case, it will immediately escalate to the employees of the Compliance Control Department, including in the Internal Referral report in writing and enters supporting documents related to TMT and performs the following:

- get additional information about the client (Information request);
- strengthen monitoring of client operations;
- review the client's risk level;
- inform the Department for Combating Economic Crimes under the General Prosecutor's Office of the Republic of Uzbekistan about SAR.

After the employee of the compliance control department revealed the necessaty of escalation of "Suspecious case", this is considered the subject of the process of rewiewing the "Suspecious case" and a "Suspecious case" will be created for "Doubtful case" in the transactions monitoring system. The "Suspicious Case" Investigation Procedure sets out the steps for conducting an in-depth investigation of an escalated "Doubtful Case". Employees of the compliance control department shall generally review the correspondence of the escalation of the "Doubtful case" to the head of compliance control department.

5.4. The process of inspecting the "Doubtful case"

5.4.1. Considering the "Suspecious case"

Once the escalation is done, employees of the compliance control department should study "Suspecious".

In the process of reviewing the "Suspecious case", the employee of the compliance control department:

- Reviewing the the Internal Referral message by the employees of the business activities who conducted the inspection of “Suspecious case”, review the customer's activity and/or all accounts;
- Review transactions holistically;
- Taken actions of additional inspection with respect to the parties who taking part in “Doubful cases”;
- Determine what further action, if any, is required to resolve the case.

5.4.2. Review of the transactions

As part of the "doubtful case" investigation process, Compliance Officers should review transaction history to gain a holistic view of customer activity.

The employee of the Compliance Control Department must review all transactions made within **three months** from the date of the transaction, which is the basis for creating a "doubtful case". In the event that several transactions are the basis for the creation of a single "doubtful case", the scope of the overall review should include all operations performed between these transactions. If necessary, the employee of the Compliance Control Department should extend the period of review of the transactions of the investigated account or the activity of the client for the purpose of comprehensive review.

A comprehensive review is carried out in the context of a “Doubful Case” and may include the following components:

- Analysis of the history of payment methods against the customer profile;
- Analyzing the payment information history which created “Doubtful case” with respect to the Fight against money laundering and typology of the Sanctions or red flag;
- Analyzing any deviations from the expected transaction activity of the customer as recorded in the customer's KYC details;
- Analyzing account activity against expected activity for the same or similar customer type;
- Identification of third parties who are customers of other branches of the bank and parties performing transactions or payers.

5.4.3. Studying the “Suspecious case”

Compliance officers apply enhanced due diligence to parties involved in transactions. If necessary, employees of the Compliance control department will conduct additional research on the parties to determine the type of industry, location and specific nature of the business. Employees of the Compliance Control Department will carry out additional studies using the following:

- Customer profile information stored in the bank (about the account, customer or external parties);
- Use of Internet search engine in public search resources and/or other open Internet search engine;
- In addition to the above searches regarding the parties, Employees of the Compliance Control Department review the thoroughness of the work performed by the employees of the Activity Line. Also, any parties and associations involved in a large number of transactions will carry out additional searches regarding the parties whose activities may indicate a high-risk type of activity or the content of activities does not correspond to the type of activity of the parties carrying out mutual transactions. As with the internal referral review process, Compliance Officers use the following principles to determine which parties will be reviewed:

- Parties whose content of activity does not correspond to the content of activity of the party sending the transactions or the business beneficiary (for example, a used car parts dealer and a merchant engaged in lumber production);
- Parties sending/receiving disproportionately large amounts of transactions or disproportionately large amounts of total funds;
- The parties who are the direct cause of the generated warning and who send/receive the transfers;
- Parties who reside or are located in a geographical location with a high level of risk;
- Parties involved in similar or repeated transactions during the review period;
- Parties who are located in a country other than the country where the bank accounts are located or who have not performed operations in the country where the bank accounts are located;
- Officials with political positions;
- Parties formed as shell companies or complex trusts with ownership form;
- Parties with an LLC or JV form of ownership where it is not customary to establish an LLC or JV form of ownership in their respective jurisdictions;
- Types of customers with a high level of risk.

5.4.4. Additional Information Request

Once transaction or customer is acknowledged as a "suspicious case", in order to reveal the risk level of the transactions and / or customer the employees of the compliance control department may request necessary and additional information to effectively implement the inspections. If the available information is not sufficient to verify the identity or existence of the customer and/or counterparties and/or If it is not possible to **sufficiently explain the economic purpose** of the transaction that created a "doubtful case" based on the results of the study, the need for additional information request will be occured. These requests are sent to the staff of the Activity Department.

In using the additional information request the following stages should be followed:

- • The employee of the Compliance control department should determine in advance what additional information is required:
  - Account information;
  - Specific questions about the activity.
- The request for additional information should be reviewed by the head of the Compliance Control Department. If deemed fit for purpose, The head of the Compliance control department sends the request for additional information to the employees of the activity department;
- The staff of the activity line analyzes and completes the request for additional information, if necessary, in consultation with the staff of the Compliance control department, requests information from others, and the completed additional information forwards the request for information to the Head of Activity for review;
- After the review by the head of the activity line, the staff of the activity line sends the completed additional information request and related information to the head of the Compliance control department;
- The head of the Compliance Control Department sends all answers to the employees of the Compliance Control Department;
- Compliance officers will use this additional information from the additional information request to continue the investigation.

Employees of the Compliance control department must receive the requested information in a timely manner in order to proceed with the investigation. If the response to the request for additional information is received in time and it is possible to close the "Suspicious Case" based

on the available information, the employees of the Compliance control department will close the "Suspicious Case".

In order to determine the mutual risk level of the client by the employees of the Compliance Control Department, A request for additional information will be sent to the staff of the Activity Department. All operations of the client will be temporarily suspended for 3 working days from the date of sending the Additional Information Request. If the client or transaction participant does not submit or refuses to submit the request for additional information, then the Bank will refuse to carry out such client's transactions and will consider measures to terminate practical business relations with the client.

The exchange of information is documented during the "Suspicious Case" review process. All requests for additional information will be directed directly to the Head of Compliance Control Department.

In case of suspicion of the accuracy of the submitted documents or other necessity, the employee of the Compliance Control Department has the right to request the submission of original copies of the documents for review.

Employees of the Compliance Control Department may take into account an interval of no more than 6 (six) weeks for the publication of the Additional Information Request. A new Request for Additional Information must be submitted if the publication deadline exceeds 6 (six) weeks.

5.4.5. Terminating the "Suspecious case"

Employee of the compliance control department should complete the inspection on "Suspecious case" after carrying out all necessary stages, including reviewing the "Suspecious case", reviewing the transactions, studying the "suspicious case" and all necessary stages including the review of the answers of the additional information requests in the respective order. After the employee of the Compliance control department conducts a review of the Suspicious Case investigation procedure, the employee of the Compliance control department gives recommendations on necessity of escalation to the head of compliance control department for closing with the sign "File is not available" or appointing with the sign SAR sending.

The employee of the Compliance control department will further choose the respective paragraph in the " Decision on the case". The conclusion, respectively, is based on the following:

- Client's business profile and country of operation;
- History of alerts generated based on customer transactions, if available;
- Reason for escalation of "Doubtful case" to "Suspicious case" level;
- Comprehensive review of general transaction data carried out for at least 3 (three) months, if available;
- Customer transaction history and any significant deviations;
- Search for negative messages;
- Relations with the field of activity;
- Other studies or reviews conducted to determine the legitimate reasons for transaction activity.

The employees of the Compliance control department explaining the recommendation forEscalationof "File is not available" or "SAR sending", while giving specific reasons supported by evidence, is responsible for preparing a draft report describing its findings. The employees of the Compliance control department should ensure the storage of the all respective approving documents in the transation monitoring systems or their separately submission.

File is not available

If the employees of the Compliance control department comes to the conclusion that transaction(s) causing "suspicious case" **does not indicate potential unusual activity**

characteristics and by means of inspection activity causing the "Doubtful case" **determines that a legal basis or business purpose exists**, it recommends to terminate the "suspicious case" according to the paragraph of "File is not available" and then completes the Status Check log. To the relevant part of the case inspection log, if necessary:

- brief information about the client's work experience and essence;
- analysis of the transaction that caused the creation of "Suspicious situation" in the context of the client's transaction history and scenario parameters;
- extenuating circumstances;
- identified red flags;
- previously "Doubtful case"s and / or "Suspecious case"s;
- negative message results;
- in case of availability, the conclusion of the previous STR or SAR;
- if available, answer conclusion of the information request;
- a description of the steps taken to investigate the customer and the transaction;
- the description of the factors and cases meaning the recommendations on escalation of "Doubtful case" to the level of "Suspecious case";
- the description of the factors and cases meaning the recommendations on terminating "Suspecious case" according to the paragraph "File is not available".

Upon completion of the "Suspicious transaction log", it will be submitted to the deputy head of the compliance control department within 1 (one) day for considering and terminating the "suspicious case" and it will be appointed as terminated in the log book of "suspicious transactions". *(The log regarding the suspicious transactions shall be formed in the "Center" system submitted by Department for Combating Economic Crimes under the General Prosecutor's Office of the Republic of Uzbekistan)*

Excalation for filling up the information of SAR

If the employee of the compliance control department comes to the conclusion that transaction causing the "suspicious case" is unusual or it is connected with the Fight against money laundering, escalation of the "suspicious case" will be recommended through filling the "log book regarding suspicious transactions" up. In case of necessity, it should include the followings of the "log book regarding suspicious transactions":

- brief information about the client's work experience and essence;
- analysis of the transaction that caused the creation of a "suspicious case" in the context of the client's transaction history and scenario parameters;
- a description of the steps taken to investigate the customer and the transaction;
- clear conclusions regarding activities deemed potentially unusual;
- identified red flags;
- previous "Doubtful cases" or "Suspecious cases";
- negative message results;
- if available, conclusion of the previous STR or SAR;
- if available, answer conclusion of the additional information request;
- a description of the steps taken to investigate the client and the transaction;
- a description of the factors and circumstances leading to the recommendation on escalation of "Doubtful case";
- a description of the factors and circumstances leading to the recommendation on escalation of "Suspecious case".

After the employees of the Compliance Control Department have disposed of the situation in accordance with the previous section, they must keep them in the "Suspicious Transactions Log" and upload the relevant supporting documents to the transaction monitoring system or submit them separately. Employees of the Compliance Control Department inform the Deputy Head of the Compliance Control Department that the investigation of the situation has been completed and there are sufficient grounds to classify the operation as a suspicious or suspicious operation.

If the client's operations are related to the legalization of proceeds from criminal activities, which do not indicate potential typical activity characteristics, after the above tasks, employees of the Compliance Control Department may impose restrictions on the operations of this client, include the client in the Bank's blacklist or terminate practical business relations with him.

5.5. Transactions in which doubtful signs related to the employees are available

All “Doubtful case”s should be reviewed and controlled in accordance with the procedure of inspection by the employees of the compliance control department as well as in case of necessity employees of the compliance control department shall carry out the inspection on “suspicious case”. Along with this, in the process of inspection of “Doubtful case”, if the employee of the Compliance control department determines that the customer being investigated or any subject of the investigation is an employee of the Business Line, the employees of the compliance control department shall deliver the “Doubtful case” directly to the deputy head of the compliance control department, he in its turn checks the “Doubtful case”. In this case, the Deputy Head of the Compliance control Department will investigate the cause and status of the alert and take appropriate action, the confidentiality of this review process must be strictly maintained. Failure to comply with confidentiality rules may result in disciplinary action up to termination of the employment contract.

5.6. Deadline of the process of “Doubtful case” and “Suspecious case”

Deadline of the process of “Doubtful case”

“Gumonli holat” yuzaga kelgandan keyin 3 (uch) ish kuni ichida tugatishlari lozim bo‘ladi. “Gumonli holat” (a) muammoli emasligi sababli tugatilgan yoki (b) qo‘shimcha tekshiruv uchun “Shubhali holat” darajasiga eskalatsiya qilinganda, ushbu “Gumonli holat” “tugatilgan” hisoblanadi. “Gumonli holat” muddatini o‘tib ketishi “Gumonli holat” yaratilgan kundan boshlab ish kunlar soni bilan hisoblanadi.

Deadline of the process of “Suspecious case”

All “suspecious case”s should be terminated within 5 (five) days after creation of these “suspecious case”, it includes the time necessary for taking the answers of additional information request. “Suspecious case” will be closed according to the recommendations related to (a) “File is not available” or (b) in case of recommendations for “SAR sending”, it will be considered “liquidated”. Expiring the date of “suspicious case” will be started from the date of creating “suspicious case”, i.e from the date of transferring from “Doubtful case” to “Suspecious case”.

Any kind of “Doubtful case”s exceeding 3 (three) working days and “Suspecious cases” which is not solved and exceeding 5 (five) working days should be excalated to the head of the compliance control department.

6. Report of SAR transactions

6.1. Adoption of decision on SAR

Upon completion of “suspicious cases”, this case includes the followigns escalating to the deputy head of the compliance control department:

- supporting documents (including subject matter (account, customer, or external parties) and counterparty investigations, adverse reporting research, transaction analysis, and other documents submitted in connection with the investigation);

- information concluded during the inspection of “Doubtful case” and (or) “Suspecious case”.

Considering the inspections on “Suspecious case”

Deputy Head of the Compliance Control Department is responsible for reviewing each case investigation conducted by the employee of the the Compliance Control Department. As part of the review, the Deputy Head of the Compliance Control Department shall assess and consider the following components of each case:

- target person (account, client or external parties) and counterparty studies;
- negative message research;
- transaction details;
- identified red flags or other potentially unusual activity;
- observations and conclusions described in the reference project; and
- mitigating circumstances, if any.

The Deputy Head of the Compliance Control Department may require the Compliance Control Department employee responsible for the investigation to provide additional information and/or answer questions regarding the case during the review. In addition, the Deputy Head of the Compliance Control Department may invite other employees of the Bank to provide advisory support when necessary.

Resolution regarding submission of SAR

After the Deputy Head of the Compliance Control Department completes the review of the escalated case and making sure that SAR should be submitted, the case shall be escalated to the Head of the Compliance Control Department. After final review and approval, the head of the compliance control department makes a decision to classify the transaction as suspicious and informs the Bank management about it. Employees of the compliance control department shall be informed about the approval of the submission of information of SAR and necessity of starting to make up its project and case management system will be closed. This case will be included in the case inspection logbook or as a “Approval date” to the transaction monitoring system.

6.2. Submitting the report on SAR

SAR files serve as the end of the transaction monitoring process when suspicious activity occurs. SARs are designed for submission of information to the Department for Combating Economic Crimes under the General Prosecutor's Office of the Republic of Uzbekistan regarding the respective expert examination conducted by the Bank and why the Bank considers that this activity is a criminal activity. Adherence to the deadlines for submission of references and compile references of SAR consistently gives chance to deliver the suspectios transactions to the bank by the law enforcement agencies for exact, short times.

6.2.1. Deadlines of SAR

After the transactions of SAR are described as suspicious, they should be sent to Department for Combating Economic Crimes under the General Prosecutor's Office of the Republic of Uzbekistan within 1 (one) working day. The respective terms which should be considered with the deadlines of submission of SAR are as follows:

Process	Stage	Deadline
Checking “Doubtful case” (Alert)	Creation of “Doubtful case” (Alert)	Within 3 (three) working days
Checking “Suspicious case” (Case)	Creation of “Suspicious case” (Case)	Within 5 (five) working days

Adoption of the decision on SAR amd sending SAR to the Department for Combating Economic Crimes under the General Prosecutor's Office of the Republic of Uzbekistan	Terminating the "suspicious case" inspection Describing the case as suspicious	Within 1 (one) working day

6.2.2. Making up the information of SAR

After SAR revealed, employee of the compliance control department develops the project of SAR. The content of each reference must be based on clear facts, but, the employees of the compliance control department should include at least the following information:

- an individual or legal entity involved in a suspicious transaction;
- ultimate beneficial owner of a legal entity;
- tools or mechanisms used to execute the suspicious transaction;
- dates of suspicious activities;
- the location of the suspicious transaction (for example, the address of several offices of the financial institution, the countries where the transaction took place);
- reasons why the bank considers the transaction suspicious;
- how the suspicious transaction was carried out.
- and others.

6.2.3. The process of submission of SAR

The resolution regarding submission of SAR should be documented in the transaction monitoring system or "Suspicious transaction log". Documents on verification of activity and SARs shall be documented by the deputy head of the compliance control department. The Board regarding the application of SAR shall inform the Board of the Bank in the written form.

Upon completion of the review by the employees of the compliance control department, the deputy Head of the compliance control department shall load the SAR through "Center" electronic transmission line of the Department for Combating Economic Crimes under the General Prosecutor's Office of the Republic of Uzbekistan.

6.3. Confidentiality of SAR and ShTTH (STR)

The employees of the bank should be care in strictly keeping the any information which is revealing the availability of SAR and ShTTH (STR). Violation of the regulation for revealing SAR or ShTTH (STR) shall cause to the responsibility established in the legislation.

If the employee of the Bank is informed about revealing of SAR or ShTTH (STR), the issue should immediately be excalated to the head of the compliance control department. The Bank limited using information related to the Combating Money Laundering, Terrorist Financing and Proliferation of Weapons of Mass Destruction including kept in the Bank archive.

The Bank shall ensure non-disclosure of the information and documents related to the Combating Money Laundering, Terrorist Financing and Proliferation of Weapons of Mass Destruction as well as shall not be entitled to inform the legal entities and individuals regarding submission of the transactions to the Department for Combating Economic Crimes under the General Prosecutor's Office of the Republic of Uzbekistan.

7. ShTTH (STR) Suspecious transactions connected with the money resources or other property

7.1. Classification of ShTTH (STR) connected with the money resources or other property

All employees of the Bank shall be responsible for preventing, identifying and reporting legalization of proceeds from criminal activities through escalating to the the head of any activity or data activity as well as compliance control department connected with Combating Money Laundering, Financing of Terrorism, Financing of Proliferation of Weapons of Mass Destruction. Due to this fact that, All employees of the Bank must be vigilant and aware of unusual activity or red flags in the fight against money laundering, proliferation of weapons of mass destruction and terrorist financing in the course of their work.

Suspecious transaction - is in the process of preparation, execution or has been completed, during the internal control, the operation is considered to be carried out in the Bank for the purpose of legalization of proceeds from criminal activities, financing of terrorism and (or) financing of distribution of weapons of mass destruction;

*According to the **paragraph 49** of the Regulation registered under No 2886* in case of availability of the following criteria and signs, this transaction is considered “suspicious”:

1. if one of the parties performing the operation is a person permanently living, staying or registered in a country that does not participate in international cooperation in the field of combating the legalization of proceeds from criminal activities and the financing of terrorism;
2. by individuals (including by several individuals in the name of one counterparty), including through money transfer systems, simultaneously or multiple times for a period not exceeding 1 month in a total amount equal to or exceeding 500 times the base calculation mechanism receiving money sent from abroad in local currency or sending money abroad;
3. sale, purchase or withdrawal of funds from international payment cards by individuals and/or individual entrepreneurs in a total amount equal to or exceeding 500 times the base calculation mechanism for a period not exceeding 1 month taken;
4. Transfer of funds to an account opened for an anonymous person outside the territory of the Republic of Uzbekistan as well as Transfer of funds to the Republic of Uzbekistan from an account opened to an anonymous person or for which there is no information about the sender;
5. transfer of funds outside the territory of the Republic of Uzbekistan to the recipient's account opened in a bank registered in an offshore area different from the place where the recipient is registered;
6. transfer of funds outside the territory of the Republic of Uzbekistan to the account or to the benefit of persons permanently residing or registered in offshore areas, or one-time or multiple transfers of funds from the account of such persons to the Republic of Uzbekistan for a total amount equal to or exceeding 500 times the basic calculation mechanism established on the day of the last transfer (arrival) (origin);
7. transactions with non-resident persons whose founders' information is not available and (or) it is not possible to obtain it through all possible methods;
8. operation related to funds or other property authorized to use funds or other property, including an attempt to transfer it;
9. Transactions that do not have the criteria and symptoms provided for in this paragraph, do not belong to the category of suspicious transactions defined by these Rules and the internal rules of a commercial bank, but are suspected by a commercial bank of being related to the legalization of proceeds from criminal activities and (or) the financing of terrorism;
10. Grants, financial assistance, loans or non-resident grants to residents by non-residents;
11. sending and receiving funds through international money transfer systems by citizens of the Republic of Uzbekistan who are in the regions where active terrorist activities are taking place (the list of countries and regions is provided by a specially authorized state body);
12. operations of persons who are internationally wanted for committing a terrorist crime (the list of persons is provided by a specially authorized state body);

13. a legal entity that has been newly established for no more than three months - if the client's turnover for purposes not in accordance with the nature of his activity is equal to or exceeds 20,000 times the base calculation mechanism;

14. purchase by individuals of the Central Bank's coins made of precious metals, measured coins of the Central Bank at the same time or for a period not exceeding 1 month, in a total amount equal to or exceeding 500 times the base calculation mechanism;

15. Transfer of funds from the customer's bank card to one or more bank cards or electronic wallets through the bank mobile application simultaneously or multiple times for a period not exceeding 30 days in a total amount equal to or greater than 500 times the base calculation mechanism;

16. receiving funds from one or more bank cards or electronic wallets to the customer's bank card at the same time or multiple times for a period not exceeding 30 days in a total amount equal to or greater than 500 times the base calculation mechanism;

17. Transfer of funds from 5 or more bank cards (e-wallets) to 1 foreign e-wallet through the bank's mobile application at the same time or multiple times for a period not exceeding 30 days;

18. Receiving funds from 1 foreign electronic wallet to 5 or more bank cards (electronic wallets) at the same time or multiple times for a period not exceeding 30 days;

19. Transfer of funds from 1 bank card (e-wallet) to 5 or more foreign bank cards or foreign e-wallets at the same time or multiple times for a period not exceeding 30 days through the bank's mobile application;

20. Incoming funds from 5 or more foreign bank cards or foreign electronic wallets to 1 bank card (e-wallet) at the same time or multiple times for a period not exceeding 30 days;

According to the risk approach of the bank if one of the following criteria and symptoms is present, this transaction is also considered “suspicious”.

1. Trading of crypto-assets bought or sold by clients through national providers in an amount equal to or greater than 500 times the base calculation base calculation engine set on the day of the transaction;

7.2. The process of identification of “suspicious transactions”

7.2.1. The process of manual inspection of “suspicious transactions”

Employees of the Bank's Activity Department identifies “suspicious transaction” of the customer for the criteria mentioned in the paragraph 7.1 of this paragraph and about such operations, he will immediately give an Internal Referral Report form in writing to the Head of the Activity Line and to the employees of the Compliance Control Department.

Employees of the Compliance Control Department are conducting further investigation of customer transactions, in order to reveal “suspicious transaction” during the current inspection by the employees of the activity, it is carried out on the basis of the criteria specified in paragraph 7.1 of this Procedure by analyzing the transactions performed by the client during the past period.

7.2.2. Inspection of the “suspicious transactions” by transaction monitoring system

The transaction monitoring system is designed to identify transactions that meet the pre-set risk level using "Suspicious Transactions" in real-time and identify situations that fall within the established criteria for suspicious and (or) suspicious transactions. Through this system, an Internal Referral message is formed on "Suspicious Transactions" related to funds or other property.

7.3. Considering “suspicious transactions”

7.3.1. Sending STR on “suspicious transactions”

In the case transactions described as “doubtful and suspecious” (according to the paragraph 48-49 of the Regulations registered under No 2886) regarding operations related to money or other property mentioned in the paragraphs 5.1 and 7.1 of the chapter 5 of this regulation are formed according to the automated program by means of transaction monitoring system or not revealed during the current inspection but should be sent all revealed STR in further inspection within 1 (one) day by analyzing by the employees of the compliance control department to the Department for Combating Economic Crimes under the General Prosecutor's Office of the Republic of Uzbekistan.

7.3.2. Monitoring of “suspicious transactions”

Employees of the compliance control department shound **monitor** all transactions causing to the “suspicious transaction” according to the stages of “***Monitoring of doubtful activity***” of the paragraph 5 of the regulation for the purpose of the existence of a legal basis and business purpose for activities that do not indicate potential unusual activity characteristics yoki noodatiy, in particular belonging to the cases connected to fight against money laundering.

7.4. Terminating the “suspicious transactions”

After the employees of the compliance control department completes the monitoring works for “suspicious transactions” in the respective order and carry out the tasks according to the paragraph (Terminating “suspicious case”) of the regulation 5.4.5.

Escalation of STR as SAR

The employee of the compliance control department comes to the conclusion that transaction causing “suspicious case” for created STR is unusual or it is particularly connected with fight against money laundering, this sent STR shall resend as a SAR.

8. The process of monitoring the transactions related to encashment of the money resources

Procedure for timely analysis of customers and their operations in connection with operations related to the cashing of funds and entities carrying out such activities has been developed in accordance with the information in the report "Structural analysis of financial flows related to the cashing of funds aimed at the commission of offenses and the legalization of criminal proceeds" of the Eurasian Anti-Money Laundering Group, Methodological recommendations of the Department for Combating Economic Crimes under the Central Bank of the Republic of Uzbekistan and the General Prosecutor's Office of the Republic of Uzbekistan as well as information from other open sources.

8.1. Concept of money laundering and money laundering

The process of legalization of proceeds from criminal activities is a set of actions aimed at giving a legal tone to the source of income obtained by illegal means, and can be carried out by the following methods:

- purchase of real estate;
- establishment of enterprises/inclusion of funds in the authorized capital of legal entities;
- withdrawal of funds from the country in order to return them later in the form of investments;
- transferring funds from the accounts of organizations to individuals for the purpose of cashing them through companies that are engaged in cashing out funds under interest loan contracts.

Cash withdrawals are not inherently criminal, but they can be linked to a number of crimes, including the legalization of the source of the proceeds of crime. The most common crimes are illegal sources of income aimed at unjustified withdrawal of cash:

- crimes in the tax field;
- crimes related to corruption;
- appropriation of entrusted property of others;
- illegal business;
- fraud.

In practice, the largest volume of criminal money flows is formed at the expense of tax and corruption crimes. For example, the field of taxation contains potential elements for the generation of criminal income, in particular, the possibility of creating fraudulent expenses. Similar schemes are used for corruption-related crimes, where cases of illegal or unjustified distribution of budget funds are common.

It is necessary to strengthen the processes of comprehensive analysis of customers' bank operations to effectively fight against illegal cashing of funds in the bank.

8.2. Schemes for cashing in proceeds of crime

Common schemes for cashing out funds obtained as a result of criminal activity are as follows:

8.2.1. Money laundering in tax crimes

Through overnight (fake) firms

One of the most common means of money laundering, such enterprises are used to commit tax crimes and embezzle budget funds. In this case, the funds transferred to the one-day enterprise account are cashed and returned to the buyer after deducting interest for one-day enterprise services (for receiving cash and issuing invoices) - from 5 to 10%. The buyer calculates the amount of VAT on the false invoice and deducts it from the total annual income. At the same time, low-quality goods (works, services) are bought with cash, because most of the money is transferred to the taxpayer. The given invoice allows the payer to artificially increase the costs of the enterprise and reduce the profit accordingly.

Through the accounts of individuals

Transfers are made from the accounts of legal entities to the accounts of individuals in the form of wages, business trip payments, financial loans, reduction of authorized capital, profits, etc. The number of such persons may be several tens or hundreds. It is possible to use nominal (dummy) natural persons, withdrawal of money from the card account is carried out by third parties (clients) using ATMs. Accordingly, these expense transactions are used to include the amounts spent by the enterprise in corporate income tax deductions.

Illegal refund of VAT

In this case, subjects of foreign economic activity overestimate the value of purchased goods in order to overpay VAT in mutual settlement with fake enterprises. Subsequently, the subject of foreign economic activity demands the state refund of the amount of VAT allegedly paid to the fake enterprise for the goods exported abroad. As a result, after the VAT refund, these funds are withdrawn in cash in order to hide them. In practice, cases of direct purchase through false invoicing are almost non-existent. Instead, a chain of 5-10 transit companies is used to hide crimes related to the fraudulent purchase of goods within the state.

Indicators describing the operations related to the commission of crimes in the field of taxation and the cashing of the resulting income

- short period of activity of the enterprise (newly opened);
- managers/founders of the enterprise: convicted persons, seriously ill or disabled persons, persons registered in psycho-narcotic dispensaries;
- the head of the enterprise is young or old;
- incompatibility of financial operations with the nature of enterprise activity;

- systematic withdrawal or transfer of funds to other accounts within a short period of time after they are deposited in the account;
- systematic withdrawal of funds through a trusted representative;
- the receipt of funds for providing a wide range of services in the absence of the main resources (technical, material) of the enterprise;
- absence or small number of employees of the enterprise;
- the transit nature of the bank account;
- use of "public" registration address;
- that the enterprise does not actually exist at the address of registration.

8.2.2. Money laundering schemes in corruption crimes

Distribution or appropriation of budget funds

Appropriation of budget funds is based on overestimation of the cost of goods, works and services. For example, a supplier organization under a state contract concludes a contract with a foreign company on increased prices. When concluding the contract, the mechanism for returning the excess funds is agreed in advance. In this case, the funds are made as loans to the accounts of legal entities controlled by officials or under separate contracts for the provision of fake services. In some cases, it is transferred to the plastic cards of individuals under the control of officials. When funds are directly appropriated, budget funds are transferred to the account of the legal entity that won the state order, after which a one-time withdrawal of funds is made. In order to hide the real beneficial owner of such enterprises, nominal (dummy) persons are registered as its leaders and founders.

Taking an illegal loan or using a budget loan for no purpose

The scheme of illegal obtaining and misappropriation of budget loans or credit funds is similar to the above schemes. Highly valued real estate objects are provided as collateral. Usually, the received funds are cashed out by enterprises or channeled into the underground economy. Bank branch managers illegally charge a few percent of the loan amount for giving unreasonable loans.

8.2.3. Fraud and pyramid schemes

Activity of financial pyramids

They are usually organized as investment funds that offer participants the opportunity to profit. "Investment" contributions can be made in cash through authorized agents and in cashless form through bank accounts, payment systems, electronic money systems. All funds are accumulated in the "pot" accounts of the financial pyramid for a certain period of time, after which they are transferred in cashless form to "transit" companies for the purpose of taking the money abroad or cashing it.

Fraudulent activity

Modern means of fraud can be fake online stores, sites that look like well-known online trading platforms, and various fake advertisements. Electronic wallets are used to pay for non-existent goods.

Indicators describing financial pyramids and fraudulent activities can be:

- contributions from individuals are made as financial assistance or free transfers;
- incompatibility of the performed operations with the types of enterprise activities;
- making contributions and transfers shortly after opening an account for a legal/individual;
- actions with signs of fraud in information obtained from open sources (financial pyramid activity);

- lack of financial and economic activity of a legal entity: employees, fixed assets, counterparties;
- the "pot" account, where the funds are collected, has a transit character;
- a complex chain of subsequent operations after receiving the funds.

At the same time, in order to improve the efficiency of the internal control system in banks and compliance with international requirements, the Central Bank, based on the "Advisory Guide for Comprehensive Analysis to Identify Money Laundering and Terrorist Financing Schemes", determines the beneficial owner of the Bank's client and introduces a guide to the identification methodology. For more details, see the "Comprehensive Analysis Methodology for Identifying AML/CFT Schemes of Appendix D" of this Regulation.

8.3. Measures aimed at preventing operations related to the cashing of funds

Preventing the involvement of the bank in illegal activities, including early detection of operations related to the cashing of funds, is one of the important tasks of the Compliance control service.

The assessment of risks in the field is carried out by the program "Oracle Business Intelligence" (Oracle BI) based on the indicators shown in Chapter 3. In this case, this program will automatically sort customers who make large amounts of money in a certain period according to criteria such as the date and address of registration, type of activity, head of the enterprise, beneficial owner and number of employees. The activity of the clients selected by the program is studied by the employee of the Compliance control service, and the increased measures are applied to the client with a high level of risk assessment, and their activity is constantly monitored.

In addition, a list of customers who made a large number of transactions through a large number of transactions during the specified period through plastic cards opened in the name of individuals is formed in the Oracle BI program, and the activities of such customers are studied by employees of the Compliance control service, and based on the results appropriate measures will be taken.

The list of entities engaged in illegal cashing of advance funds, information about their managers and beneficiaries is included in the list of "Black List Customers" of the bank's automated system (ABS). lib, when entities on this list and their managers contact the bank, their operations are automatically blocked. Such operations can be carried out only with the permission of the Compliance Control Service.

At the same time, in the process of daily monitoring, employees of the Compliance control service are engaged in the sale of highly liquid goods, receiving funds on preferential loans, carrying out operations that do not have a clear economic nature, as well as the level of risk. it is necessary to constantly monitor and study the operations of customers highly rated by the employee.

8.4. Limits of depositing and withdrawing cash from the account by individuals

In order to combat the legalization of proceeds from criminal activities, the financing of terrorism, and the financing of the distribution of weapons of mass destruction, the Bank applies the following measures to the transactions related to cash carried out by individuals:

1. 1. The employees of the activity department will form a customer questionnaire to determine the risk profile when opening an account for non-resident natural persons, conduct an interview with him and take measures to obtain documents confirming the legality of the sources of funds, as well as provide explanations to each customer about the existing restrictions. increases;

2. Quantitative limit on withdrawal of cash foreign currency from the accounts of non-resident individuals is in **1 month – 10 thousand US dollars** or **in one year – 120 thousand US dollars**;

3. The following quantitative limits are set for currency exchange and account deposit transactions. Documents confirming the legality of the source of funds are required for transactions exceeding this limit:

- • during **30 days** of foreign exchange transactions and depositing money into accounts by resident individuals - transactions exceeding the equivalent of **100,000 US dollars**;
- • during **30 days** of non-resident individuals transferring money to their accounts and carrying out any currency exchange operations - transactions in the amount of more than **10 thousand US dollars** equivalent.

Employees of the activity line require information about the source of funds requested from individuals directly from the client. If the information about the source of funds is not substantiated or is rejected by the client, the transaction will be rejected.

9. The procedure for monitoring operations related to crypto-assets

9.1. Activity of the crypto-assets

The development of the payment services market leads to an increase in the number of applicants for licenses granting the right to operate a payment system operator and a payment organization.

This is, in its turn, demanding ensuring the stable operation of payment systems and the rights, freedoms and legal interests of payment service providers and payment service users, regular control and monitoring of the activities of payment services market participants.

It should be noted that according to the Financial Action Task Force (FATF) report "Virtual Assets: Signs of Money Laundering":

- • the majority of crimes in the field of cryptoassets are predicate crimes and crimes related to the legalization of criminal proceeds;
- • that criminals use crypto-assets to avoid economic sanctions and support terrorism;
- • among these types of crimes, the most widespread is the sale or purchase of prohibited (narcotic) substances for crypto-assets, or their use in the process of legalization of criminal income is recorded as a final conclusion.

However, there are cases of illegal purchase and sale of crypto-assets using the services provided by banks and payment organizations. In particular, individuals who have organized illegal crypto-asset trading are actively using the following payment services:

- money transfer services through bank accounts of individuals;
- service of money transfers through bank cards;
- service of money transfer from bank cards to electronic wallets;
- cross-border money transfer service.

9.2. Establishing a risk rating of customers carrying out operations related to crypto-assets

Clients carrying out operations related to crypto-assets through national providers will be included in the **high-risk** category and will be subject to increased monitoring..

If the client has not carried out operations related to crypto-assets through national providers within the last one year from the day of the operation, he will be removed from this risk category.

9.3. Monitoring operations related to crypto-assets

It is determined that the citizens and legal entities of the Republic of Uzbekistan may carry out operations on the purchase, sale and (or) exchange of crypto-assets only through (licensed) national providers in accordance with the procedure established by legislation. Therefore, the Bank implements the following measures regarding operations related to crypto-assets:

- • refuses to carry out operations on crypto-assets through unlicensed providers and ceases practical business relations with such clients;
- • formation of a monitoring system of internal and cross-border operations and operations carried out through a virtual terminal using all types of payment instruments (bank card, electronic wallet, etc.) aimed at detecting illegal operations on crypto assets. Herein:
  - Employees of the activity line constantly monitor the operations carried out with the payment code "MSS 6051";
  - Determines the sub-payment codes that are provided for implementation by this payment code and restricts the implementation of operations through them;
  - Notifies Compliance Officers of customers attempting to transact through these restricted payment codes.
- • Development and implementation of additional internal criteria for identifying suspicious transactions related to crypto-assets and reporting to Department for Combating Economic Crimes under the General Prosecutor's Office of the Republic of Uzbekistan about suspicious transactions. Herein:
  - Employees of the activity department constantly monitor the transactions of customers dealing with crypto-assets through "national operators";
  - Informs the employees of the Compliance Control Department about crypto-assets bought and sold through national providers in an amount equal to or exceeding 500 times the amount of the base calculation set for the day of the transaction.
- In the event that the share of the volume of transactions through terminals not related to crypto-assets (points of sale, etc.) is significantly larger than the total volume of transactions:
  - Employees of the activity line provide all the necessary files in this regard to the employees of the Compliance Control Department;
  - Employees of the Compliance Control Department will carry out in-depth studies on this situation;
  - If it is determined that transactions were made through these terminals (points of sale, etc.) through exchanges dealing with illegal crypto-assets, the Compliance Control Department will take measures to block this terminal.

9.4. Setting restrictions on customers carrying out operations related to crypto-assets.

Given that there is a high probability that crypto-asset transactions are used in the legalization of criminal proceeds, that crypto-assets are used by criminals to avoid economic sanctions and support terrorism, and that narcotics are sold or bought for crypto-assets, or used in the process of legalizing criminal proceeds obtained from them in order to verify the relevance of the above-mentioned activities, the Bank establishes restrictions:

- • transactions of crypto-assets bought and sold through national providers equal to and above 500 times the base valuation mechanism in one day are stopped using the transaction monitoring system software. As a result of investigations, this operation is allowed if it is carried

out on the basis of other economic interests, not related to the fight against the legalization of proceeds from criminal activities, the financing of terrorism and the financing of the distribution of weapons of mass destruction.

At the same time, in order to improve the efficiency of the internal control system in banks and to comply with international requirements, the Central Bank, on the basis of the "Recommended Guidelines for the Activities of Commercial Banks in the Operation of Accounts in Trading Enterprises for Transactions Carried Out Using Electronic Payment Instruments", determines the beneficial owner of the Bank's client and introduces guidelines on the identification methodology. For more details, see the "Bank's Methodology for Settlements with Trading Enterprises for Transactions Carried Out Using the Client's Electronic Payment Instruments of Appendix F" of this Regulation.

10. Quality control

10.1. Overview on quality control

The quality control review process is carried out in order to determine whether transaction monitoring for "Doubtful case" (Alert) and "Suspecious case" (Case) has been effectively implemented and documented to the Bank in a manner that meets the Bank's standards.

The Quality Control review process for transaction monitoring is based on a two-pronged approach for "Doubtful case" (Alert) and "Suspecious case" (Case) respectively.

Quality control inspection for "Doubtful case" (Alert) is carried out by the appointed employees of the Bank during the on-site visit based on the information collected during the specified period. Quality control inspection for "Suspecious case" (Case) is carried out **once every six months** by the head of the "Financial Transactions Monitoring Department" of the Compliance Control Department.

Quality control audits can be performed by a qualified third party (eg, an external auditor, etc.). In this case, the head of the Compliance Control Department will check the compliance and qualifications of the third party in advance.

10.2. Deadline of the execution of the quality control

Quality control inspection is carried out every six months by the head of the "Financial Transactions Monitoring Department" of the Compliance Control Department. If the Quality Control review is not completed within the required time frame, the reviewer will notify the Head of Compliance by e-mail as soon as possible, indicating the reasons for the delay (for example, time or resource constraints).

10.3. Quality control inspection process

Upon the “Suspecious case”s have been reviewed and completed, the completed “Suspecious case”s shall become into the one part of the quality control inspection. Depending on quality control inspection (“Doubtful case” and “Suspecious case”) for transaction monitoring, each designated Quality Control Inspector is responsible for conducting an inspection in accordance with the following procedure:

Sampling choosing

To select a quality control sample, the inspector must request a list of all suspicious transactions created for the period during which the quality control will carry out inspections.

From the list downloaded through the transaction monitoring system, sample "Doubtful cases" and "Suspicious cases" should be selected for review by Quality Control during a certain period. (that is, cases that were terminated during the previous period).

Quality control assessment map

After selecting the sample, the Quality Control Inspector will analyze the description, conformance of the statement and supporting documents of each sample.

Transaction review

The quality control reviewer should review the transactions entered for the following purposes:

- Confirm that the information in "Doubtful Case" and "Suspicious Case" match customer and transaction data;
- Confirm that the check of the transaction history was carried out correctly in accordance with this Procedure.

Document review

The quality control inspector will also review supporting documents for the following purposes:

- confirm that any linked web pages and files can be viewed (for example, the identification data of the subject (account, customer or external parties), such as company information, location, contact information);
- confirmation that searches for negative messages are carried out in an appropriate manner and that the results are evaluated for relevance and importance;
- confirmation that the necessary supporting documents are correctly uploaded to the transaction monitoring system or submitted separately.

Considering the final part of the cases

The quality control inspector inspects the final part used for the following purposes:

- Confirm that information is used correctly, is not overly general, and matches the details of “Doubtful case” and “Suspicious Case”;
- Verify that “Doubtful case” and “Suspicious Case”, negative message search and links and citations corresponding to transaction details are correct;
- Confirm that each case is based on supporting evidence;
- Confirmation that the final statement reflects the full summation of the “Doubtful case” and “Suspicious Case” details based on the study and comprehensive profile of the individuals and legal entities involved.

10.4. 10.4. Quality control rating and overall assessment

The Quality Control Examiner assigns a Quality Control Score of Pass or Fail for each sample reviewed using the following criteria:

- If there is no error, a “successful” quality control rating will be given to any kind of sample;
- A “Fail” quality control rating is given to any reviewed sample that has a single error;
- If the quality of the data or the evidence provided does not have enough information to support a final decision on a “Doubtful case”, the Quality Control Reviewer may issue a “Fail”;
- If there are unspecified cases of "Suspicious case" (that is, if not informed about SAR within established time), regardless of the number of errors, during the review period, Quality Control is considered failed and the head of the Compliance Control Department will have to take appropriate measures immediately.

10.5. The next step is to review the quality control

All Quality Control reviews are documented on the Quality Control Assessment Map, logged and presented to the case reviewer.

The Quality Control Auditor shall maintain a record of the meetings held, a list of participants and specific topics discussed, and "Quality Control Assessment Maps" completed in

accordance with the record keeping procedure. *(See the paragraph 13 regarding keeping the records)*

Possible follow-up actions based on the results of the quality control review include at least the following:

- training for the case examiner;
- conducting additional research or requesting additional documents to support the investigation.

10.6. Creating the quality control report

Quality control report *(See the attachment No 1 "regarding quality control report")* is made up according to the results of quality control inspections and submitted to the head of the compliance control department. The following information shall be included in the quality control report:

- the number of examined samples;
- number of Quality Control Indicators assessed as "successful";
- number of Quality Control Indicators assessed as "failed";
- identification of serious Compliance risks;
- determine the needs of retraining of employees;
- the results of the quality control inspection will be included in the agenda of the meeting of the Bank Council, which is expected for discussion.

11. Transactions monitoring system management

The head of the Compliance Control Department monitors and identifies suspicious transactions in a timely manner and conducts "Doubtful cases" and "Suspicious cases" at an optimal level through the transaction monitoring system, which is one of the important parts of the Bank's Compliance Program, at least once a year Responsible for setting and managing rule scripts and limits.

11.1. 11.1. Rule script management

The Compliance Control Department shall establish and maintain a list of Rules.

In the event that there are any typologies or rule scenarios not covered by the Bank's new products, services and processes, in order to identify potential risks, it will be necessary to add and change the rule script over time, as well as delete the existing rule script if it is deemed inappropriate.

Employees of the Compliance control department are required to forward the rules script to the Deputy Head of Compliance Control Department and then to the Head of Compliance for review or review of the relevant grounds. After the Head of the Compliance Control Department approves the results of the review, the Compliance Control Department staff updates the relevant rule scripts in the transaction monitoring system.

11.2. Limits management

The limits of the rule scenario are initially determined quantitatively and qualitatively based on the requirements of regulatory authorities, expert opinions and the Bank's risk appetite, will be corrected taking into account market conditions and the effectiveness of creating "Doubtful Case".

The results of the analysis carried out by the employees of the Compliance Control Department and the basis for decision-making should be documented and registered in the transaction monitoring system. It is necessary for the deputy head of the Compliance control department to review the results of the analysis and deliver them to the head of the Compliance

control department. The Chief Compliance Officer approves the limits to be set and adjusted for rule scenarios, and then the Compliance Officer reflects the appropriate limit in the transaction monitoring system.

12. Information exchange

Department for Combating Economic Crimes under the General Prosecutor's Office of the Republic of Uzbekistan has right to take information necessary for the implementation of measures to combat money laundering, terrorist financing, and the financing of proliferation of weapons of mass destruction from Automated information system of the bank and database of the Bank in a written form and for free.

The Bank provides additional information on written requests of the Department for Combating Economic Crimes under the General Prosecutor's Office of the Republic of Uzbekistan.

In the event of a request from an authorized body of a foreign state participating in the fight against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction, The Department of Combating Economic Crimes under the General Prosecutor's Office of the Republic of Uzbekistan submits a relevant request to the Bank through the Central Bank. Based on such a request, the bank will provide the requested information to the Department for Combating Economic Crimes under the General Prosecutor's Office of the Republic of Uzbekistan.

Such requests should be sent immediately to the Bank's Compliance Control Department. The Office of Compliance is responsible for responding to legal process or other requests for information and forwarding such requests to government agencies.

The Bank keeps records of received requests and submitted responses, including supporting documents submitted in accordance with the Bank's document retention requirements.

13. Record keeping

In order to limit to use the documents used in the activity of the compliance control department (Correspondence with the Central Bank and the Department for Combating Economic Crimes under the General Prosecutor's Office of the Republic of Uzbekistan, including electronic messages to the Department for Combating Economic Crimes under the General Prosecutor's Office of the Republic of Uzbekistan, electronic forms of customer questionnaires, magazines, etc.) such documents and their list are stored directly by the Compliance Control Department (responsible employee) in a specially equipped room or in a safe for the periods specified in the legislation, but at least for 5 (five) years. Only employees of the Bank Compliance Control Department have the right to use these records.

Banks shall limit access to information related to the fight against money laundering, terrorist financing, and the financing of proliferation of weapons of mass destruction, including documents stored in the archives of commercial banks, and ensure its non-distribution, as well as legal and physical do not have the right to inform individuals that their transactions have been reported to a specially authorized state body.

The Bank ensures that the information obtained during the performance of internal control tasks is not disclosed by its employees (or is not used for personal purposes or in the interests of third parties).

Transaction data must be recorded in such a way that the details of the transaction can be reconstructed if necessary.

After the storage period ends, the documents are submitted to the Bank's archive in the prescribed manner.

14. Attachments

Information	Title	File
Attachment A	The form of Internal Referral Notification	
Attachment B	The form special logbook	
Attachment C	Logbook in soft copy	
Attachment D	Comprehensive Analysis Methodology for Identifying AML/CFT Schemes	
Attachment E	Methodology for identifying transactions related to illegal cashing of funds of legal entities.	
Attachment F	Bank's methodology for settlements with trading enterprises for transactions carried out using the client's electronic payment instruments	