evocaBANK

FINANCIAL CRIME PREVENTION POLICY

Code POL23-0001-15 INT		Edition 03
Prepared by		Approved by
Internal Financial Monitoring Division	Management Board minutes N29 of 12/08/2024 Chairman of Management Board Karen Yeghiazaryan _____	Supervisory board minutes N11 of 28/08/2024 Chairman of Supervisory Board Jose Maria Moreno de Barreda _____

Application area	Internal Financial Monitoring Division
Unit in-charge of revision	Internal Financial Monitoring Division
Effective date	29/08/2024
Expiration date	

Content

1. Purpose

This Policy sets forth the principles, requirements and procedures of preventing financial crimes in the Bank.

2. Definitions

- **Bank** – Evocabank CJSC
- **Policy** – Financial Crime Prevention Policy
- **FC** – Financial crime
- **IFM division** – Bank's Internal Financial Monitoring Division
- **CB** – Central Bank
- **Business** – all subdivisions engaged in customer service process.
- **Sanction** – the sanctions imposed by the United States of America (Office of Foreign Assets Control, Bureau of Industry and Security), European Union, United Kingdom, United Nations Organization.
- Other definitions used herein will be applied within the meaning specified in relevant Armenian law.

3. The Policy

3.1. The FC prevention policy sets forth minimum standards and control arrangements enabling the Bank to mitigate the FC risk.

3.2. The Bank carries out its activities in line with anti-money laundering, counter-terrorism financing and proliferation of weapons of mass destruction law, regulations.

3.3. The Policy has been developed on the basis of the RA law on Anti-money laundering, combating of terrorism financing and proliferation of weapons of mass destruction, as well as other regulations based on the mentioned law and international practice.

3.4. This Policy has been developed by the IFM division and approved by the Bank Supervisory Board.

3.5. The Supervisory Board also exercises general control over the introduction and implementation of the Policy.

3.6. The Bank's CEO will ensure the adoption, efficient implementation and current oversight of the Policy.

3.7. The IFM division will review the Policy at least once a year, as needed and at the request of the CBA. Each Policy amendment upon approval by the Bank Supervisory Board will be submitted to the CBA not later than in seven-day period. The CBA may request making amendments to the Policy which should be done by the Bank in a month-period along with submission to the CBA within a seven-day period of the amendments to the Policy and relevant internal legal acts.

3.8. The Policy sets forth a risk-based approach to combating financial crimes which means that control framework and processes are different depending upon risk category.

3.9. The Policy applies to all Bank structural and territorial subdivisions, without exceptions.

3.10. Based on this Policy, the IFM division may adopt procedures and guidelines detailing certain business processes.

3.11. The businesses shall include in their legal acts provisions ensuring compliance with the minimum requirements set forth herein.

4. FC definition

FC is banking sector abuse for illegal purposes. It includes the following crimes:

- **Money laundering –** conversion, transfer of criminally obtained assets, concealment or distortion of its real nature, origination, location, ownership type, its movement, title, acquisition or retention or utilization or disposal (if known that the asset has been obtained as a result of criminal activities) meaning to conceal or distort the criminal origin of the asset or assist any person in order to avoid responsibility for the committed crime.
- **Sanctions evasion –** deliberate circumvention of sanctions imposed by the United States of America (Office of Foreign Assets Control, Bureau of Industry and Security), European Union United Nations Organization's Security Council, United Kingdom.
- **Tax evasion –** illegal activities in which natural persons or legal entities avoid paying their legal taxes.
- **Bribery –**giving, offering, getting cash or other valuables in order to affect a certain decision or action.
- **Corruption –** abuse of power by an official.
- **Financing of terrorism** – attempts or actions meant to support terrorist acts. Terrorism causes large losses and damages (including human) to the society; its purpose is to affect the public or the government.

- **Financing of weapons of mass destruction** – provision of funds for purchasing, transportation, storage of nuclear, chemical, biological weapons or associated materials and technology through violation of international conventions, laws and obligations.
- **Fraud** –acquiring property or other assets through fraudulent actions.

5. Three Lines of Defense

5.1. For efficient risk management, three lines of defense are defined per roles, responsibilities and goals:

1. The first line of defense or risk-owner is the business providing services to natural persons and legal entities who is responsible for preparation, implementation and observance of regulations, procedures detailing their activities on the basis of minimum criteria set forth herein,
2. The second line of defense is the roles and responsibilities of IFM division and Internal controls who are responsible for setting minimum compliance requirements, their on-going monitoring, customer's due diligence, analysis of signals of FCs, CBA reporting on suspicious transactions.
3. The third defense line is the audit unit who independently assesses Bank's risk management and oversight framework. It is performed through regular audit of first and second lines of defense.

6. Assessment of Bank Risks Associated with Money Laundering and Terrorism Financing

6.1. The IFM Division will identify, assess and at least once a year review its potential and current risks associated with money laundering and terrorism financing, proliferation of weapons of mass destruction, and relevant sanctions. In order to address these risks, the IFM Division will take into consideration all risk factors and undertake individual actions by risk type and risk category. The IFM Division will assess the inherent risks and control arrangements in order to identify the residual risk level.

7. Customer Due Diligence

7.1. The Bank will assess FC-related risks of each customer and perform customer due diligence depending upon risk category prior to establishing business relations or throughout the entire period of business relationship.

7.2. The Bank will identify its customers on the basis of independent and reliable sources: verifying their identity through paper or electronic documents supplied with photos and issued by the governments in the cases as follows:

1. Establishment of business relations,
2. Conclusion of occasional transaction (one-off related-party transactions), whose amount equals or exceeds AMD 400 000 unless the law sets forth more stringent provision,
3. While identifying the customer, suspicions are arisen as to the reliability or completeness of previously obtained information (including documents),
4. Suspicions are arisen in relation to possibility of money laundering or financing of terrorism.

7.3. In case of customer (including authorized person or beneficial owner) identification, the Bank may rely on the data obtained from other financial or non-financial institutions or a person as a result of customer due diligence whenever the following conditions are met:

1. The Bank should bear ultimate responsibility for customer due diligence,
2. The Bank should directly obtain from other financial and non-financial institutions or a person customer identification data,
3. The Bank should take sufficient actions in order to make sure that the other financial or non-financial institution or natural person:
   - Is entitled and in a position to immediately supply upon request the information obtained as a result of customer due diligence, including document copies,
   - Is subject to proper regulation and oversight in terms of combating money laundering and financing of terrorism, besides, it has efficient procedures in place for conducing customer due diligence and information retention as set forth in the law and relevant legal acts arising from the aforementioned law.,
   - Is not domiciled or residing in or is not from non-compliant countries or territories.

7.4. The Bank may choose not to pursue the customer due diligence except customer identification and verification

if there is a suspicion of money laundering or terrorism financing and the IFM division, customer service units have reasonable grounds to suspect that the customer due diligence will lead to identification of suspicions activities. In this case, the customer service employee will send a relevant signal to IFM Division, and the latter will file a report with the CBA on suspicious transaction or business relation.

7.5. The Business should determine all the documents acceptable for establishing business relations or conducting an occasional transaction. In particular, acceptable documents are: government-issued valid identification document with photos: RA passport, RA special passport, other national passports, identification card for natural persons, state register extract for legal entities and sole proprietors.

7.6. The identification documents should be submitted to customer service employees in original copies or certified copies validated as a true copy by a competent specialist. The documents may also be obtained from official databases provided by third parties and acceptable by the Bank, for instance Nork information center or other official electronic register.

7.7. All documents submitted by the customer should be scanned and stored in Customer folders and kept in acceptable for Bank systems.

7.8. IFM division should clarify any differences between the customer's documents and information from official database. If it is impossible to identify the reasons of such discrepancies or if the reasoning is unacceptable for the Bank, establishment of business relations with the customer shall be prohibited.

7.9. The business will not be entitled to establish business relations with a customer prior to obtaining of necessary information for conducting due diligence. In exceptional cases IFM division may allow establishing business relations before the due diligence if IFM division has made as assessment of the sanction risk. The Bank may not establish or continue business relations if it is impossible to conduct enhanced due diligence. The Bank may identify the customer at a maximum of seven days upon setting business relations if the risk is effectively addressed and it is essential to avoid interruption of the ordinary course of business.

7.10. The Bank should prepare and implement a policy and procedures to address any specific risks associated with non-face-to-face transactions or business relations, including the need to identify and verify the customer; these regulations should be applied when establishing business relationships and conducting ongoing due diligence. When setting non-face-to-face business relationships, the Bank as part of customer due diligence should request the first payment be made in the customer's account opened with the financial institution, which is:

1. Entitled and in a position to immediately upon request provide information collected as part of customer due diligence, including document copies,
2. Subject to regulation and oversight for combating money laundering and terrorism financing, besides, it has effective procedures in place for conducting customer due diligence and information storing,
3. Not domiciled or residing in or from any non-compliant country or territory.

7.11. Prior to setting business relationships with all the customers and related parties (owners, beneficial owners, executives, authorized representatives), the Bank should consult the list of sanctions issued by the European Union, US Office of Foreign Assets Control, Bureau of Industry and Security, United Nations Organization, United Kingdom, lists of politically exposed persons (PEP) and the lists provided by the CBA, other lists containing negative information. The Bank should check the customer's first name, last name, other well-known names, trade name, beneficial owner, title holder, authorized entities against the mentioned lists while identification of designated persons should be confirmed or denied by IFM division.

7.12. In case of exceptions to minimum requirements for customer due diligence as set forth in the Policy, the Business should submit to IFM division an explanation and risk-based justification, obtain a written approval from IMF division for setting or continuing business relationships. Analyses, approvals, rejections or exceptions should be duly maintained.

7.13. The Business prior to setting business relationships, will collect the following information and documents:

7.14. **Natural persons**

1. Full name (as shown in submitted documents)
2. Month, day, year of birth (as shown in submitted documents)
3. Registration or residence address, if any
4. Citizenship (as shown in official document)
5. Personally identifiable information (as shown in submitted documents)
6. Sources of funds (as indicated in documents - for high-risk customers and whenever needed)
7. Purpose and intended nature of business relationships

8. Center of vital interests for foreign individual customers,
9. Existence of authorized person. The Business should identify and verify all persons entitled to act on behalf of the customer, and make sure the power of attorney is issued by the customer.
10. Intended account activity. When setting business relationships, the Business should find out the intended account activity. The Business should make distinction between the cases when the intended account activity is evident (for example, mortgage loans) and the cases when the intended activity is not evident and additional explanation by the customer is needed.

7.15. **Sole proprietors**

1. Full name (as shown in submitted documents)
2. Date, month, year of birth (as shown in submitted documents)
3. Registration or residence address
4. Trade name
5. Citizenship (as shown in submitted documents)
6. Personally identifiable information (based on submitted documents)
7. Month, day, year of registration of sole proprietor (SP) (based on submitted documents)
8. SP TIN (based on submitted documents)
9. Sources of funds (as indicated in documents for high-risk customers and whenever needed)
10. Purpose and intended nature of business relationships
11. Area of activities. The Business should find out the nature of customer's activities. The nature of activities and customer's transactions should match each other. The Business should identify the customer's main partners.
12. Existence of authorized person. The Business should identify and verify all persons entitled to act on behalf of the customer, and make sure the power of attorney is issued by the customer.
13. Intended account activity. When setting business relationships, the Business should find out the intended account activity. The Business should make distinction between the cases when the intended account activity is evident (for example, mortgage loans) and the cases when an additional clarification is needed from the customer since the intended activity is not evident.

7.16. **Legal entities**

1. Legal entity's full name (as shown in submitted documents)
2. Office address (based on submitted documents)
3. State registration number (based on submitted documents)
4. Trade name
5. Registration address (as shown in submitted documents)
6. Month, day, year of registration (as shown in submitted documents)
7. Charter (based on submitted documents)
8. Company executives' identification data (based on submitted documents)
9. Authorized person's identification data (based on submitted documents)
10. Beneficial owner's identification data
11. Area of activities. The Business should find out the customer's business profile. The business profile and customer's transactions should match each other. The Business should identify the customer's main partners.
12. License if necessary
13. Organizational and legal form (based on submitted documents)
14. Organizational structure
15. List of owners except for open joint-stock companies
16. Main financial indicators (based on submitted documents)
17. Main partnering countries
18. Main partners
19. Sources of funds (as indicated in documents for high-risk customers and whenever needed)
20. Purpose and intended nature of business relationships
21. Existence of authorized person. The Business should identify and verify all persons entitled to act on behalf of the customer, and make sure the power of attorney is issued by the customer.
22. Intended account activity. When setting business relationships, the Business should find out the intended account activity. The Business should make distinction between the cases when the intended account activity

is evident (for example, mortgage loans) and the case when an additional clarification is needed from the customer since the intended activity is not evident.

7.17. **Public Organizations**

1. Full name (as shown in submitted documents)
2. Trade name if any
3. Legal status (as shown in submitted documents)
4. Registration address (as shown in submitted documents)
5. Office address (as shown in submitted documents)
6. Registration number (as shown in submitted documents)
7. Month, day, year of registration (as shown in submitted documents)
8. Area of activities. The Business should find out the customer's business profile. The business profile and customer's transactions should match each other. The Business should identify the customer's main partners.
9. Decision on incorporation (based on submitted documents)
10. Structure
11. Charter (based on submitted documents)
12. List of founders and identification data
13. Composition and identification data of board of trustees
14. Executive's or other governance bodies' identification data, including on a collective basis
15. Authorized person's identification data (based on submitted documents)
16. Beneficial owner's identification data
17. Sources of funds (based on submitted documents)
18. Purpose and intended nature of business relationships
19. Existence of authorized person. The Business should identify and verify all persons entitled to act on behalf of the customer, and make sure the letter of authorization is issued by the customer.
20. Intended account activity. When setting business relationships, the Business should find out the intended account activity. The Business should make distinction between the cases when the intended account activity is evident (for example, mortgage loans) and the case when an additional clarification is needed from the customer whenever the intended activity is not evident.

7.18. **Fund**

1. Full name (based on submitted documents)
2. Legal status (based on submitted documents)
3. Registration address (based on submitted documents)
4. Office address (based on submitted documents)
5. Registration number (based on submitted documents)
6. Month, day, year of registration (based on submitted documents)
7. Actual location
8. Area of activities. The Business should find out the customer's business profile. The business profile and customer's transactions should match each other. The Business should identify the customer's main partners.
9. Decision on incorporation (based on submitted documents)
10. Fund structure
11. Charter (based on submitted documents)
12. Founders list and identification data
13. Composition and identification data of board of trustees
14. Executive's or other governance bodies' identification data, including on a collective basis
15. Authorized person's identification data (based on submitted documents)
16. Beneficial owner's identification data
17. Sources of funds
18. Purpose and intended nature of business relationships
19. Existence of authorized person. The Business should identify and verify all persons entitled to act on behalf of the customer, and make sure the power of attorney is issued by the customer.
20. Intended account activity. When setting business relationships, the Business should find out the intended account activity. The Business should make distinction between the cases when the intended account activity

is evident (for example, mortgage loans) and the case when an additional clarification is needed from the customer since the intended activity is not evident.

7.19. **Foundation**

1. Full name (based on submitted documents
2. Legal status (based on submitted documents)
3. Registration address (based on submitted documents)
4. Office address (based on submitted documents)
5. Registration number (based on submitted documents)
6. Month, day, year of registration (based on submitted documents)
7. Area of activities. The Business should find out the customer's business profile. The business profile and customer's transactions should match each other. The Business should identify the customer's main partners.
8. Decision on incorporation (based on submitted documents)
9. Structure
10. Rules and regulations (based on submitted documents)
11. Registration certificate issued by the CBA (based on submitted documents)
12. Founders list and identification data
13. Foundation manager's identification data (register, charter, share extract issued by depository if the foundation manager is a CJSC)
14. Authorized person's identification data (based on submitted documents)
15. Beneficial owner's identification data
16. Sources of funds
17. Major investors, including by country
18. Purpose and intended nature of business relationships
19. Existence of authorized person. The Business should identify and verify all persons entitled to act on behalf of the customer, and make sure the power of attorney is issued by the customer.
20. Intended account activity. When setting business relationships, the Business should find out the intended account activity. The Business should make distinction between the cases when the intended account activity is evident and the case when an additional clarification is needed from the customer since the intended activity is not evident.

7.20. **Cooperative society**

1. Name (based on submitted documents)
2. Registration address (based on submitted documents)
3. Actual place of operations
4. Charter (based on submitted documents)
5. State registration number (based on submitted documents)
6. Month, day, year of registration (based on submitted documents)
7. Area of activities. The Business should find out the customer's business profile. The business profile and customer's transactions should match each other. The Business should identify the customer's main partners.
8. Decision on incorporation (based on submitted documents)
9. Founders list and identification data
10. Authorized person's identification data (based on submitted documents)
11. Beneficial owner's identification data
12. Sources of funds
13. Purpose and intended nature of business relationships
14. Existence of authorized person. The Business should identify and verify all persons entitled to act on behalf of the customer, and make sure the power of attorney is issued by the customer.
15. Intended account activity. When setting business relationships, the Business should find out the intended account activity. The Business should make distinction between the cases when the intended account activity is evident (for example, mortgage loans) and the case when an additional clarification is needed from the customer since the intended activity is not evident.

7.21. **For a government body or local self-governance bodies:**
1. Full official name of the government body or self-governance body
2. Country.

7.22. The Business should find out the source of funds and if needed, source of wealth, supporting the information with documents and whenever applicable, by acquiring the following information:
1. The countries from which they expect to collect receivables,
2. Which legal entities or natural persons will transfer funds to the customer's account,
3. What is the volume of transferred funds.

7.23. The Business should make a distinction between the cases when the source of funds is evident (e.g. salary projects) and the case when an additional clarification is needed from the customer since the source of funds is not obvious. Whenever the source of funds is unusual, the Business should get additional information so that the source of funds is acceptable for the Bank.

7.24. The Bank will evaluate all customers as involving low, medium or high risks.

7.25. In case of low risk, simplified due diligence should be conducted,

7.26. In case of medium risk, due diligence is needed.

7.27. In case of high risk, due diligence is required.

7.28. Whenever a customer risk is high, prior to establishing business relations, it is necessary to obtain IFM division's approval. A change in customer's risk rating should be supported by relevant explanation.

7.29. Low risk-rated entities are:
1. From the perspective of combating money laundering and financing of terrorism, effectively controlled financial institutions,
2. government agencies, local self-governance bodies, state non-commercial entities, community governance bodies, except for bodies and organizations located in non-compliant countries or territories. Besides, low risk-rated items are:
3. Life insurance policies where the annual insurance premium does not exceed the amount of four hundredfold of the minimum salary or the lump-sum insurance premium does not exceed the amount of a thousand-fold of minimum salary;
4. Insurance policies made as part of pension programs unless they contain a denial clause and the contract may be used as collateral;
5. Payments to the Republic of Armenia state budget or community budgets, or for public services,
6. Payments related to salary, pension or other well-known sources of social allowances.

7.30. The risk is assessed as **medium** when high or low risk criteria are absent.

7.31. **High risk criteria include:**
1. Domestic and foreign politically exposed people, their family members, and otherwise related parties,
2. Embassies, consulates and representation offices,
3. Legal entities and natural persons widely using cash,
4. Non-for-profit organizations (charitable organizations, public and religious organizations, funds, etc., except government non-business entities),
5. Dealers in precious stones and precious metals,
6. Organizations with unnecessarily complex structure of ownership (three layers, let alone the customer and beneficial owner),
7. Entities engaged in nuclear energy sphere,
8. Entities engaged in mining,
9. Wealthy natural persons (whose average monthly account balance is USD 1 million or more or an equivalent amount in another currency),
10. Persons domiciled or residing in non-compliant countries or are from these countries,
11. Non-residents or foreign legal entities
12. Individuals whose transactions are linked to virtual currencies,
13. Beneficiaries of life insurance policies,
14. Legal entities who are engaged in individual asset management,
15. Customers using personalized banking services,
16. Customers posing significant reputational risk to the Bank,
17. Legal entities having non-resident or foreign owners

18. Casinos, online casinos companies engaged in bookmaker activities,
19. Crowd funding platforms, entities engaged in wire transfer services.

7.32. **Prohibited customers**

1. Sanctioned natural persons and legal entities,
2. Entities entitled to issue bearer shares,
3. Entities engaged in military activities, operations relating to illegal weapons or ammunition,
4. Entities engaged in activities associated with drugs and psychotropic substances,
5. Entities engaged in adult entertainment services,
6. Banks registered in offshore jurisdictions,
7. Shell banks and organizations,
8. Organizations operating without relevant license,
9. Organizations providing virtual currency services,
10. Natural persons and legal entities in relation to which there are facts or well-grounded suspicions that they are engaged in financial crimes.

7.33. **Prohibited accounts**

1. It is prohibited to open anonymous accounts, accounts under fictitious names,
2. Accounts having only numbers, letters or other arbitrary symbols.

7.34. In the case of availability of several criteria, the risk is categorized as high. In the event of availability of high-risk criterion, the Bank can assess it as medium if as a result of comprehensive and well-documented analysis it concludes that these risks are effectively addressed and mitigated. In case of occurrence of any risk criterion in the course of business relationships with the customer, the customer service employee and IFM division should revise the risk category undertaking customer due diligence commensurate with the newly rated risk. All risk rating changes will be approved by the IFM Division.

7.35. In the case of low risk, a **simplified due diligence** should be conducted, which constitutes a limited application of customer due diligence process implying that during customer identification and verification the following information will be collected:

1. For natural persons: first name, last name, patronymic (if any) and ID data,
2. For legal entities: company name and identification number (state registration, registration number, etc.),
3. For government bodies and local self- governance bodies: full official name.

7.36. Where the risk is low, the following simplified measures should be undertaken:

1. Verify the authenticity and reliability of information (including documents) pertaining to the transaction or business relationships, based on the information provided by the customer,
2. Compare the sources, movement and volumes of funds circulating in various transactions per unit timeline only in case when they exceed the maximum amounts reasonable from the perspective of the customer's business profile,
3. Find out the existence of links between customers, transactions and business relations only in cases of identification of links between medium (standard) or high-risk customers, transactions or business relationships.

7.37. In the event of a medium risk, a **customer due diligence** is conducted in order to have a clear picture of the customer through obtaining and analyzing customer identity and business profile information (including documents) with application of risk-based approach, to cover the following:

1. Identification and verification of the customer identity (including its authorized representative and beneficial owner),
2. Clarification of the purpose and intended nature of the transaction or business relationship,
3. Ongoing due diligence of the business relationship.

7.38. In the case of medium risk, the following actions should be taken:

1. Verify the authenticity and reliability of information pertaining to the transaction or business relationships supplied by the customer (including documents), if necessary, obtaining of the information from limited access or publicly available sources, inquiring competent bodies and other reporting entities as well as foreign partners;
2. Compare the sources, movement and volumes of funds circulating in various transactions per unit timeline;
3. Find out the existence of links between customers, transactions and business relations ;
4. Verify the compliance of the transaction or business relationship with customer's business profile;

5. Find out the source of the customer's incomes;
6. Undertake other measures as specified in internal legal acts.

7.39. In case of high risk, **enhanced due diligence** should be conducted, which is the application of advanced process of customer due diligence by the Bank in which case in addition to the actions prescribed under standard due diligence, it is also necessary to perform at least the following:

1. Obtain the approval of IMF division prior to setting business relationships as well as in cases when later on it is identified that the customer or beneficial owner is characterized as posing high-risk or the transaction or business relationship imply such criteria;
2. Find out and document the source of customer's incomes;
3. Examine as thoroughly as possible the preconditions and purpose of the transaction or business relationship;

7.40. In the case of high risk, advanced measures should be performed as part of ongoing due diligence on business relationship:

1. When verifying the authenticity and reliability of information (including documents) supplied by the customer in relation to the transaction or the business relationship, the Bank will request necessary information (including additional documents), also obtaining information from limited access or publicly available sources, inquiring competent bodies and other reporting entities as well as foreign partners;
2. When comparing the sources, movement and volumes of funds circulating in various transactions , the Bank will choose the longest possible period or several comparable periods;
3. When finding out the links between customers, transactions and business relationships, it will conduct a multi-stage analysis, including the one designed to identify possible indirect links;
4. When verifying the customer's business profile with any transaction or business relationship, it will request information (including documents) fully supporting the actions taken as part of the aforementioned;
5. When finding out the source of customer's incomes, it will request information (including documents) supporting their legitimacy;
6. Undertake other actions as prescribed in internal legal acts.

The Bank will conduct regular customer due diligence pursuant to the RA law on Combating money laundering and financing of terrorism.

7.41. The Bank may determine other period differing from those mentioned in the Law if as a result of comprehensive and well-documented analysis it concludes that these risks are effectively addressed and mitigated. The outcomes of the Bank's analysis will be reported to the CBA.

7.42. The information obtained as a result of customer identification and verification should be updated at least once a year.

7.43. As a result of regular due diligence, the Bank will make sure that:

1. The previously obtained customer information is true, including the identify of beneficial owner, and risk rating;
2. The customer's transactions and the announced nature and purpose of business relationships match each other;
3. There is a sufficient explanation for the discrepancies in the customer's transactions and announced nature and purpose of business relationships;
4. There is a change in announced nature of business relationship and business purpose;
5. There is a change in the sphere of activities,
6. There is a sanction risk.

7.44. The following events may also serve as a signal for conducting customer due diligence:

1. The customer moves from the country of registered activities to another, higher-risk jurisdiction;
2. Change in beneficial owner;
3. Owner changes;
4. Essential changes in source of customer's funds;
5. Business sphere changes;
6. Change in organizational and legal form;
7. Obtaining of essential negative information about the customer;
8. The customer's risk exposure becomes more severe;
9. Required due diligence at the initiative of IFM or as a result of IFM analysis;

10. When suspicions arise as to the reliability of previously obtained information and documents.

8. FC Signals

8.1. In the event of an unusual transaction, all the Bank employees are entitled and obliged to submit to IFM division signals of financial crime in cases when the transaction appears unusual, has no economic purpose, and is not consistent with the business nature and purpose announced by the customer. All the reports on unusual transaction shall be analyzed by IFM division in a 90-day period. As a result of it, the IFM division will make a decision as to whether or not this transaction or suspicious business relationship should be reported to the CBA.

9. Conducting Analysis, Disclosure of Suspicious Transactions and CBA Reporting

9.1. The IFM division will implement risk-based monitoring in order to identify suspicious transactions. To this end, the Bank should install an automated or non-automated monitoring software to comply with the Business size and nature, making it possible to monitor all bank transactions. High-risk customers and transactions with high-risk countries (territories) will be subject to enhanced due diligence. All signals received from the mentioned sources as well as the analysis initiated by IFM division should be implemented by IFM division within a 15-day period. The results of analyses will be retained irrespective of the fact whether a suspicious transaction, business relation report is filed with the CBA or not.

The IFM division will start the process of analyzing the transaction or business relationship both in case of receiving internal and external signals when:

1. There are signals generated by the transaction monitoring software,
2. There are signals sent to IFM by Bank employees,
3. CBA requests for information about the customer,
4. Bank customer-related directives issued by law enforcement bodies,
5. Signals received from publicly available sources,
6. At the initiative of IFM, when:
    - There is a potential similarity between the customer's personal data or the data of other party to the transaction and persons engaged in terrorism or proliferation of weapons of mass destruction or the personal data of other persons mentioned in CBA directives;
    - The monitored situation totally or partially corresponds with criteria or characteristics of suspicious transactions or business relationships;
    - The logic, movement (dynamics) of the concluded or proposed transaction or business relationship or other circumstances give basis to assume that it can be implemented for money laundering or financing of terrorism;
    - There are other circumstances showing the existence of the suspicious transaction or business relationship as specified in internal legal acts.
    - Others.

9.2. If as a result of monitoring, the transaction or business relationship is not qualified as suspicious and no report is submitted on suspicious transaction or business relationship, then the grounds of refraining from qualifying the transaction or business relationship as suspicious, conclusions made, the course and results of the analysis should be documented and retained by the Bank.

9.3. If based on the analysis outcomes, the head of IFM division concludes that there are sufficient grounds to suspect money laundering through the transaction or business relationship, then the head of the division should report to the CBA on suspicious transaction, business relationship on the day of arising suspicion or by 12 a.m. the next day.

10. Suspension and Rejection of Suspicious Transactions or Business Relationships, Freezing of Assets of Persons Associated with Terrorism or Proliferation of Weapons of Mass Destruction

10.1. Where a suspicion arises regarding money laundering or financing of terrorism, the IFM division is entitled to **suspend** the transaction or business relationship for up to 5 days while in case of CBA relevant directive, it is obliged to **suspend** them for 5 days immediately reporting to CBA on suspicious transaction or business relationship. The CBA decision on suspension of suspicious transaction or business relationship should be made without delay upon receipt of the report from the Bank. In case of failure to notify the CBA on the need for

extension of the suspension period, the suspension will be cancelled. The decision of the Bank or CBA on suspension of transaction or business relationship prior to the end of the suspension period may be deemed invalid only at the CBA initiative or Bank recommendation unless there is a need for further suspension of the transaction or business relationship.

10.2. Where it is impossible to perform customer due diligence or a relevant directive is issued by the CBA, the Bank – IFM division, customer service division - shall **reject** the implementation of the transaction or establishment of business relations and consider qualifying it as suspicious. The transactions rejected by customer service employees will be recorded in the rejected transactions register.

10.3. Where it is impossible to implement customer identification after establishing business relationship and/or a relevant directive is issued by the CBA, the Bank - IFM division, customer service division - shall terminate the business relationship and the IFM division will consider qualifying it as suspicious. The transactions rejected by customer service employees will be recorded in the rejected transactions register.

10.4. The assets directly or indirectly owned or controlled by persons included in United Nation's Security Council resolutions or lists published on their basis as well as lists provided by the CBA shall be immediately subject to freezing by IFM division when there is sufficient identifying information or when it was not possible to confirm the absence of identifying information, these assets are subject to **freezing** by IFM division without prior notice. It is prohibited to directly or indirectly make funds, economic resources or financial or other related services available to or for the benefit of the persons involved in terrorism or proliferation of weapons of mass destruction. In the event of freezing the assets of the persons or entities involved in terrorism or proliferation of weapons of mass destruction, the Bank without delay shall qualify the transaction or business relation as suspicious and file a report to the CBA on suspicious transaction or business relationship.

10.5. Unfreezing of funds and assets may be performed by CBA only.

10.6. The asset shall not be subject to freezing if it is owned by a bona fide third person, i.e. the person who when handing over the asset was not and could not be aware that the assets would be used or were intended to be used for criminal actions, including financing of terrorism or proliferation or financing of weapons of mass destruction as well as the person who when handing over the asset was unaware or could not be aware of the criminal origin of these assets.

11. Information Retention

11.1. The Bank should retain the information collected during customer due diligence, including documents irrespective of the fact whether the transaction or business relationship is continuing or suspended, including:

1. Customer identification data, including data about account number and account activity as well as business communication data,
2. All necessary information about interstate and international transactions or business relationships (including customer's (and the other party to the transaction) name, registration address (if any) and place of residence (location), nature of the transaction, timing, amount and currency, also account number and type (if any), which will be sufficient in order to reconstruct the entire picture of the transaction or business relationship,
3. Information on suspicious transactions or business relationships as well as the course and results of monitoring (conducted analysis) of the transactions or business relationships not qualified as suspicious,
4. Results of assessment of potential and current risks associated with money laundering and terrorism financing,
5. Information specified in wire transfers.

11.2. The mentioned information and documents should be kept at least for 5 years after the completion of the transaction or end of business relationships.

11.3. Reports on transaction monitoring, signals, analyses, unusual transactions, suspicious transaction or business relationship shall be kept confidential. Other Bank employees, except for IMF employees, Management board chairman, Management Board members, Bank Supervisory Board members, should not have access to the mentioned information.

11.4. The information retained by the Bank should be sufficient for providing each time of thorough and comprehensive information about the customers, transactions or business relationships requested by CBA or investigating bodies or public participants in the proceedings.

11.5. The mentioned information should be duly available to competent supervision and investigative bodies, public participation proceedings as well as to auditors.

11.6. The stated information may be collected and retained in hard copies or electronically.
11.7. The information subject to retention should be recorded so that, if necessary, it would be possible to recover the employee personal data who has conducted customer due diligence or other actions aimed at acquiring information subject to retention.
11.8. The Bank should ensure the safety and confidentiality of the retained information.
11.9. The Bank, its employees, executives are prohibited from notifying the person in question about CBA reporting or providing it with other information, or receiving CBA information request.
11.10. The Bank shall submit to the CBA the information (including confidential) associated with money laundering and terrorism financing.
11.11. The IFM division in a timely manner will respond to the CBA inquiries regarding Bank customers and transitions.

12. Wire Transfer Transparency

12.1. When implementing a wire transfer, the Bank should obtain and keep the following information, attaching it to the payment instruction accompanying the wire transfer:
1. Full name of the sender and recipient,
2. Sender's and recipient's account numbers (if not available, a single reference number accompanying the remittance),
3. Sender's personal data or ID data, or address or date of birth and location for natural persons or personalized number (state registration, registration number, etc.) or location for legal entities.

12.2. The above-mentioned actions will not be applied in:
1. Funds transfer and mutual settlements between financial institutions,
2. Transactions implemented using credit, debit or prepayment cards if all the communications serving as basis for performing such transaction and account treatment (accompanying communication) already contain card information. Exceptions are the cases when the transaction refers to withdrawal of cash from automated teller machines, payment for goods and services; while the following case should be included in the aforementioned group of transactions when credit, debit or prepayment cards are used to transfer funds through any money transfer system.

12.3. In case of transferring funds, the Bank is acting as an intermediary or transfer recipient, the Bank should have in place effective risk-based policy and procedures in order to identify and take relevant measures (including rejections or suspension) to the wire transfers failing to include the above-mentioned information.
12.4. The Bank should exclude making any changes in information contained in payment instruction thus avoiding disclosure of the transaction in question by another financial institution.

13. Establishment of Correspondent Relations

13.1. In a correspondent banking or similar relationships with foreign financial institutions the Bank in addition to customer due diligence requirements, should:
1. Collect sufficient information in order to understand the nature of the respondent institution's business and based on public or other reliable information, assess the business reputation of the respondent institution and the quality of its supervision, including the information as to whether the financial institution has been or is currently subject to money laundering or financing of terrorism investigation or regulatory action,
2. Assess the respondent institution's anti-money laundering and terrorism financing controls in order to ascertain that they are sufficient and effective,
3. Prior to establishing correspondent relationship, it is necessary to obtain IFM division's approval,
4. Ascertain that the respondent institution:
   - In the event of transit accounts, conducts due diligence on the customers having direct access to financial institution's accounts and whenever requested, may provide necessary information regarding the due diligence on these customers,
   - Does not allow use of its accounts by shell banks,
   - The financial institution is prohibited from establishing or continuing correspondent or similar relationship with shell banks.

13.2. Prior to establishing correspondent or similar relationship, the relevant Bank unit will submit to IFM division the correspondent bank registration documents, license, owner composition, AML/FT policy, completed Wolfsburg questionnaire, other documents when necessary.

14. Monitoring

14.1. IFM division shall regularly but not later than once every 6 months perform monitoring of at least the customer accounts opened with Bank structural and territorial subdivisions as well as the relevant transactions. Its purpose is to ascertain that FC prevention arrangements are in place and effective. The Business should have regulations in place to address the challenges identified as a result of monitoring.

15. New Products

15.1. IFM division jointly with the Business will assess the FC risk associated with provision of new types of services or application of new methods of their provision using new or advanced technology. IFM division will be involved at the initial stage of project discussions. IFM division will consider the risks and suggest control mechanisms for containment of FC risk associated with the product in question. The Business should obtain the IFM division's written approval prior to launching the new product.

16. Training

16.1. IFM division will organize the training of all relevant Bank employees: Supervisory Board, executive body, IFM division, those engaged in customer service and internal audit functions as well as other competent employees engaged in combating FC.

16.2. Employee training is aimed at:

1. Understanding the FC countering laws and regulations,
2. Understanding the risk associated with FC, how it is possible to identify and address it,
3. Understanding their own role and responsibility in combating FC,
4. Understanding the consequences of incompliance.

16.3. IFM division will prepare training materials commensurate with the business model and product size, make sure the training materials are reviewed on an annual basis and updated and that the training course is effective.

16.4. Customer service employees at least twice a year will undergo training on combating FC. All new employees will undergo training on combating FC in three months after their recruitment. Other employees will undergo training once a year.

16.5. The conducted training materials, documents on training attendees' data and participation details will be recorded and retained for at least 5 years.

17. Audit

17.1. The Bank's Audit unit will ensure independent assessment of efficiency of FC prevention controls in first and second lines of defense. The internal audit should make sure that the Bank's operations are in compliance with the requirements of the Armenian law on combating money laundering and financing of terrorism, other legal acts regulating its implementation. The Audit unit will include the review of FC prevention process in its annual plan. The challenges identified by the Audit unit will be discussed with IFM division. Addressing the mentioned problems is the responsibility of IFM division.

17.2. The Bank will invite external audit in the manner specified by the CBA, as requested by the latter or on its own initiative, to audit the state of introduction and efficiency of regulations combating money laundering and terrorism financing.

17.3. The Bank will invite an external auditor at its initiative or as requested by the CBA. The external auditor will review the compliance with the requirements of regulation on combating money laundering and terrorism financing and efficiency of their implementation.

17.4. If the CBA requires performing external audit, the Bank within a month-period will invite an external audit company whose audit opinion will be submitted to the CBA within a week-period.

18. IFM Division, Structure, Goals

18.1. The Bank has Internal Financial Monitoring Division who is responsible for drafting FC prevention policy, other internal legal acts arising from the policy, introduction of control arrangements, their monitoring aimed to assess their efficiency, providing the Business with FC-related advice, conducting of transaction monitoring, providing mandatory information to the CBA and reporting on business relationships, making decisions on qualifying the transaction as suspicious, on suspending, rejecting or terminating the transaction or business relationship, on

taking a final decision on freezing the assets owned by persons associated with terrorism or proliferation of weapons of mass destruction, as well as performance of other duties as ascribed under the mentioned legal acts.

18.2. Employees of IFM division will have relevant qualification in line with CBA requirements and professional compliance criteria.

18.3. IFM division will have direct and immediate access to all information (including documents) obtained and retained by the Bank.

18.4. IFM division is independent in performing its duties specified herein and has a Bank senior management status. IFM division is entitled to directly present to the Supervisory Board the Bank's challenges associated with prevention of money laundering and terrorism financing, as well as participate in discussions of issues relating to prevention of money laundering and terrorism financing.
The IFM division will approve the Financial Crime Prevention Policy , other relevant internal legal acts.

18.5. IFM division may inform the executive body and the Supervisory Board on qualifying the transaction or business relationship as suspicious, on rejecting or suspending it, freezing the assets owned by entities associated with terrorism or proliferation of weapons of mass destruction only after reporting to the CBA on suspicious transaction or business relationship, making a decision on suspending, rejecting or terminating the transaction or business relationship, on freezing the assets owned by entities involved in terrorism or proliferation of weapons of mass destruction.

18.6. The role and responsibilities of IFM division shall not be ascribed to internal audit subdivision or any of its employees.

18.7. Employees of Internal Financial Monitoring division will be hired and dismissed by the CEO with the consent of the Supervisory Board.

19. Mandatory Reporting and Reporting on Suspicious Transactions and Business Relationships

19.1. IFM division will supply the CBA with a report on suspicious transaction or business relationship, and information subject to mandatory reporting.

19.2. The suspicious transaction or business relationship report will be filed regardless of the transaction amount. The cashless transactions amounting to AMD 20 million or above and cash transactions amounting to AMD 5 million and above as well as equivalent foreign currency amounts are subject to mandatory reporting.

19.3. The details of suspicious transaction or business relationship reporting, information subject to mandatory reporting, exceptional transactions, and information contained in the report, as well as timelines for report filing will be specified in individual guidelines developed by IFM division.

20. Reporting

20.1. On a quarterly basis, IFM division will submit a report to the Management Board and Supervisory Board to include the following information:

1. Number and brief description of of transactions subject to mandatory reporting,
2. Number and brief description of suspicious transactions and business relationships,
3. Number and summary description of transactions and business relationships analyzed but not qualified as suspicious,
4. Number and brief description of suspended, rejected or terminated transactions and business relationships, amount of each suspended transaction or business relationship,
5. Size of frozen asset related to terrorism financing,
6. Cases of incompliance with this policy and other relevant legal acts resulted from actions by Bank employees,
7. Letters, investigations and/or other related information from CB regarding AML issues,
8. Other information specified in internal legal acts.