

	QUALITY MANAGEMENT SYSTEM	MANUAL 14#6		
	“ACBA-CREDIT AGRICOLE BANK” CJSC POLICY OF FINANCIAL SECURITY	<i>Edition date 11/09/14</i>	<i>Edition 1</i>	<i>Page 1 of 12</i>

PURPOSE

The purpose of “ACBA-CREDIT AGRICOLE BANK” CJSC policy of financial security (hereinafter referred to as “the Policy”) is to define “ACBA-CREDIT AGRICOLE BANK” CJSC (hereinafter referred to as “the Bank”) principles of ensuring of financial security, the Bank’s activities on combating money laundering and terrorism financing and approaches to the meeting of the requirements of the international sanctions and the USA “Foreign Account Tax Compliance Act” (FATCA).

APPLIATION SCOPE

The provisions of this Policy relate and are applicable to the management bodies and managers and employees of all subdivisions of the Bank.

RELATED DOCUMENTS

RA Criminal Code	
RA Law “On Combating Money Laundering and Terrorism Financing”	
“Regulation on the Minimal Requirements Stipulated for the Reporting Entities in the Field of Combating Money Laundering and Terrorist Financing” (approved by the Board of the Central Bank of Armenia, decree No. 279-N, dated 07.10.2014)	
Regulation of Financial Security Division of “ACBA-CREDIT AGRICOLE BANK” CJSC	ACBA 55 REG 15
"ACBA-CREDIT AGRICOLE BANK" CJSC order on maintenance of combating money laundering and terrorism financing and international sanctions	ACBA 72 ORD 37

DEFINITIONS AND CONCEPTS

“Law” – RA Law “On Combating Money Laundering and Terrorism Financing”

“Property” – according to Part 4 of Article 103.1 of the Criminal Code of the Republic of Armenia: any type of material goods, tangible or intangible objects of the civil right, including financial means (cash), securities and property rights, documents or other means evidencing the property rights or interests, interests received or accrued to the property, shares or other income, as well as related and beneficial rights

“Money laundering” (ML) – deed specified in Article 190 of the Criminal Code of the Republic of Armenia: the conversion or transfer of property, knowing that such property is proceeds of crime, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of the predicate offence to evade the legal consequences of his actions; or the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of, property, knowing that such property is proceeds of crime; or the acquisition, possession, use or disposition of property, knowing, at the time of receipt, that such property was proceeds

“Terrorism financing” (TF) – deed specified in Article 217.1 of the Criminal Code of the Republic of Armenia committed by natural or legal persons: terrorism financing – direct or indirect provision or collection of property in any way, realizing that it will be or may be used, fully or partially, for terrorism or hostage taking, by a terrorist organization or a terrorist, or provision of financial services, realizing that these services are directed for terrorism or hostage taking, or their results will be used by a terrorist organization or a terrorist

“Terrorism-related person” – any individual or organization included in the list of individuals and organizations published by the UN Security Council or designated by the Authorized Body, as well as persons suspected, accused, or convicted for terrorism

“Authorized Body” – Central Bank of the Republic of Armenia

“Senior Management” – Financial Security Division of the Bank, entitled to make decisions and take actions on behalf of the Bank on issues related to preventing money laundering and terrorism financing

“Transaction” – a transaction concluded between the Bank and a customer or an authorized person,

	QUALITY MANAGEMENT SYSTEM	MANUAL 14#6		
	“ACBA-CREDIT AGRICOLE BANK” CJSC POLICY OF FINANCIAL SECURITY	Edition date 11/09/14	Edition 1	Page 2 of 12

as well as between a customer or an authorized person and other persons through the Bank. Any action giving rise to rights and obligations based on or resulting from a certain deed may also be deemed as a transaction

“Occasional transaction” – a transaction, which does not give rise to obligations between the customer and the Bank to provide recurrent services (no business relationship is established)

“Affiliated occasional transactions” – occasional transactions of the same nature with the participation of the same person, which are performed within 24 hours

“Business relationship” – recurrent services provided by the Bank to the customer, which are not limited to one or several occasional transactions. Business relationship with the Bank does not include those activities with the Bank, within which the Bank for its own needs carries out operations different from the ones legally designated for banks

“Customer” – a person establishing or involved in business relationships with the Bank, as well as a person, who offers the Bank to conclude an occasional transaction or to render other services aimed at carrying out the transaction

“Beneficial owner” – a natural person who is not a party to the business relationship or transaction, and on whose behalf or for whose benefit the customer acts, and (or) who ultimately owns and (or) controls the customer or the person on whose behalf the transaction is being carried out. The beneficial owner of a legal person is the natural person, who exercises factual (real) control over the legal person or transaction (business relationship), and (or) for whose benefit the business relationship or transaction is being carried out. A natural person may be recognized as the beneficial owner of a legal person, if such natural person:

- a) owns 20 percent or more of the voting stocks (equities, shares; hereinafter: stocks) of the given legal person; or, by force of his/her participation in or under the agreement concluded with the legal person, has the ability to predetermine its decisions;
- b) is a member of the management and (or) governing body of the given legal person;
- c) acts in agreement with given legal person, based on common economic interests.

“Authorized person” – a person authorized to carry out a transaction or to undertake certain legal or factual actions in the course of business relationship upon the assignment and on behalf of the customer; including the person, who conducts representation by a power of attorney or by any other legal authorization of the customer; as well as the person who actually acts on behalf or upon the assignment of the customer, or undertakes factual actions at the expense or for the benefit of the customer without a power of attorney

“Legal entity” – an organization or an institution having the status of a legal entity by the legislation of the Republic of Armenia and (or) a foreign country, as well as a legal organization, not having the status of a legal entity by the foreign legislation

“Business profile of a customer” – a complete set of data (understanding) of the Bank about the sources of income, profile, influence and significance of the customer; the presence and expected dynamics, scope, and areas of relevant business relationships and occasional transactions; the presence, identity, and nature of affiliation of authorized persons and beneficial owners

“Know Your Customer (KYC) principle” – a principle, adopted in the international practice, which assumes a need for the collection of the customer’s identification details, checking of the customer’s business description, regular update of the information, collected about the customer, and it is applied for the proper study of the customer and transactions, performed by the latter

“Other party to the transaction” – other participant of the transaction being carried out by the customer, who provides (transfers) the cash or other assets proceeding from the transaction, or to whom such cash or assets are addressed

“Customer’s due diligence” – In order to obtain a proper understanding about the customer by the Bank, a process of obtaining and analysis of the information (including documents) about his/her identity and business description, by applying the approach based on risks, which includes:

- a) customer’s (including the authorized person’s and beneficial owner’s) identification and checking of identity,
- b) detection of the purpose of the business relationship and the envisaged nature,
- c) current proper study of the business relationship.

“Risk” – a circumstance, evidencing of danger of ML/TF and its probability, which can be described by the countries or geographical location, type of customers, type of transactions or business relationship, type

	QUALITY MANAGEMENT SYSTEM	MANUAL 14#6		
	“ACBA-CREDIT AGRICOLE BANK” CJSC POLICY OF FINANCIAL SECURITY	<i>Edition date</i> 11/09/14	<i>Edition 1</i>	<i>Page 3 of 12</i>

of services or by other criteria

“High risk criterion” – criteria established by this Law, by normative legal acts of the Authorized Body, as well as by internal legal acts of the Bank, which evidence the high likelihood of money laundering and terrorism financing, including:

- the politically exposed persons and their affiliated persons, i.e. their family members or a person affiliated with them in another way (father, mother, husband, wife, grandmother, grandfather, sister, brother, children, parents of husband/wife), being the possible or available customers or real beneficiaries,
- persons (including financial institutions), which are located or residing in the high risk countries (in particular, in Non-compliant countries or territories, Off-shore countries or territories, countries, subject to international sanctions, countries with high corruption risk, or are from such countries or territories),
- all complex transactions or transactions with unusually large amounts,
- transactions or business relationship with unusual terms, the economic or other legal purposes are not clear.

The availability of high risk criterion in a transaction or business relationship, in cases, established by the Authorized Body and the Bank, may be defined with the combination of the specified criteria.

“Customer’s enhanced due diligence” – a broader application of the process of the customer’s due diligence, when besides the actions, specified by the due diligence, at least the following is also required:

- a) to receive the approval of the Senior Management prior to the establishment of a business relationship with the customer, to continue the business relationship, as well as in cases, when in the future it is detected that the customer or the beneficial owner is defined by the criterion of high risk, or the transaction or business relationship contain such a criterion,
- b) to initiate relevant measures to detect the income and the source of property of the customer,
- c) to scrutinize the preconditions and the purpose of the transaction or business relationship,
- d) in case of politically exposed person, to perform a current supplementary observation.

“Low risk criterion” – criteria established by this Law or normative legal acts of the Authorized Body, which evidence the low likelihood of money laundering and terrorism financing, including:

- financial institutions efficiently supervised in terms of combating money laundering and terrorism financing,
- state bodies,
- local self-governed bodies,
- state non-commercial organizations,
- state-owned organizations.

The exception are the bodies or organizations, located in Non-compliant countries or territories, Off-shore countries or territories, countries, subject to international sanctions, countries with high corruption risk. The availability of low risk criterion in a transaction or business relationship, in cases, established by the Authorized Body, may be defined with the combination of the specified criteria.

“Customer’s simplified due diligence” – a limited application of the customer’s due diligence by the Bank, when performing the identification and checking the identity, the following information shall be collected:

- a) for natural persons – first name, last name and the details of the identification document,
- b) for legal entities – name and identification number (state registration number, residence number, etc.),
- c) for state bodies and local self-governed bodies - full official name.

“Politically exposed person” – an individual, who is or has been entrusted with prominent state, political, or public functions in a foreign country or territory. The list of politically exposed persons does not include persons of medium or low rank, performing public functions. The politically exposed persons are namely:

- a) heads of the state or government, ministers or deputy ministers;
- b) members of the parliament;
- c) members of supreme courts, constitutional courts or other high rank judiciary, whose decisions are not subject to appeal, except for special circumstances;
- d) members of audit courts or of the boards of central banks;
- e) ambassadors, charges d’affaires and high rank officers of the armed forces;
- f) outstanding members of political parties;

	QUALITY MANAGEMENT SYSTEM	MANUAL 14#6		
	“ACBA-CREDIT AGRICOLE BANK” CJSC POLICY OF FINANCIAL SECURITY	<i>Edition date 11/09/14</i>	<i>Edition 1</i>	<i>Page 4 of 12</i>

g) members of administration, management, or supervisory bodies of state-owned organizations.

“Off-shore country or territory” – a country or a territory, included in the list of off-shore countries or territories, published by the Authorized Body

“Non-compliant country or territory” – in accordance with the lists, published by the Authorized Body, a foreign country or territory not applying or improperly applying the international requirements of the combating of ML/TF

“Country under international sanction” – a country, in regard to which the international sanctions are applied, in particular, by the European Union, France or the USA (OFAC)

“Country with high corruption risk” – a country, which has a high corruption risk, according to the classification of “Corruption Perceptions Index”, by Transparency International organization

“Center of vital interest” – the location, where the family or economic interests of an individual are concentrated. The location of family or economic interests is the place, where the house (apartment) of the individual is located, where the individual and his/her family reside and his/her (family’s) main personal and family assets is maintained, or the place of performance of core economic (professional) activity

“Suspicious transaction or business relationship” – a transaction or business relationship when, in cases established by this Law, the guidelines established by the Authorized Body, and the internal legal acts of reporting entities, or in other cases, it is suspected or there are sufficient grounds to suspect that the assets involved in the transaction or business relationship proceed from crime, or that such assets are linked to terrorism financing, as well as when the funds or other assets are linked to or intended for use by terrorist organizations or individual terrorists for the purpose of terrorism

“Criterion of a suspicious transaction or business relationship” – a situation or an alarm evidencing the probability of ML/TF, established by the legal acts of the Authorized Body, as well as by the internal legal acts of the Bank

“Typology” – possible schemes describing the logic and frequency of actions and (or) steps directed to ML/TF, specified by the legal acts of the Authorized Body or by the internal legal acts of the Bank

“Suspension of business relationship or transaction” – blocking for a certain time period, in the manner established by this Law, of the factual and legal movement of funds or other assets, which are the subject of a suspicious business relationship and (or) transaction

“Rejection of business relationship or transaction” – non-implementation of actions, intended for carrying out a suspicious business relationship or transaction

“Termination of business relationship or transaction” – termination of implementation of business relationship or transaction

“Freezing of funds” – blocking for a certain time period, in the manner established by this Law, of the factual and legal movement of funds of the persons linked to terrorism, including blocking of direct or indirect possession, use or management of that property, as well as ban of any business relationship (including financial services), or blocking of execution or approval of occasional transactions

“Shell bank” – a bank which, while being registered in a state, does not have an actual place of presence and activity in the territory of that state and is unaffiliated with other operating financial institutions

“Transit account” – a correspondent account, opened with the Bank, which is directly used by the customer of the correspondent financial institution to perform transactions on his/her behalf

“FATF” – intergovernmental body, the purpose of which is to develop and spread the national and international policies on combating ML/TF (The Financial Action Task Force)

“International sanctions” – international embargoes, applied to the types of goods and (or) business sectors and persons of countries or territories, requirements to freeze the property

“FATCA” – USA“Foreign Account Tax Compliance Act”

UNIT ONE

CHAPTER 1. GENERAL PROVISIONS

1.1. This Policy has been developed in compliance with the Law, “Regulation on Minimal Requirements Stipulated for the Financial Institutions in the Field of Combating Money Laundering and Terrorist Financing” approved by the Board of the Authorized Body, and with the requirements of other legal acts,

	QUALITY MANAGEMENT SYSTEM	MANUAL 14#6		
	“ACBA-CREDIT AGRICOLE BANK” CJSC POLICY OF FINANCIAL SECURITY	<i>Edition date</i> 11/09/14	<i>Edition 1</i>	<i>Page 5 of 12</i>

FATF standards, international best practice, and regarding FATCA – also in compliance with the intergovernmental agreement.

1.2. The process of financial security in the Bank is implemented for the following main purposes:

- Implementation and application of “Know Your Customer” principle in the Bank,
- Application of the approach based on ML/TF risks,
- Detection of suspicious transactions and business relationship and their reporting to the Authorized Body,
- For the maintenance of international sanctions – application of data processing systems of customers and transfers,
- Adherence to FATCA requirements,
- Organization of training of the Bank’s personnel on financial security,
- Organization of proper maintenance of the information and documents on financial security.

1.3. The implementation and control of the process of financial security in the Bank is performed by the Financial Security Division, which performing its activities is guided by the RA legislation, international standards and requirements, Bank’s charter, this Policy, Regulation of Financial Security Division of “ACBA-CREDIT AGRICOLE BANK” CJSC [ACBA 55 REG 15](#), "ACBA-CREDIT AGRICOLE BANK" CJSC order on maintenance of combating money laundering and terrorism financing and international sanctions [ACBA 72 ORD 37](#), as well as by other internal legal acts of the Bank, instructions of the Bank’s Board, orders and instructions of the Chief Executive Officer of the Bank.

1.4. The Financial Security Division:

1.4.1. performing the functions, specified by this Policy and internal legal acts adopted on its basis, is independent and has the status of senior management,

1.4.2. has the right to directly submit to the Bank’s Board the issues occurred in the financial security sector of the Bank, as well as to participate in the discussions by the Bank’s Board on the financial security issues.

1.5. The Financial Security Division has direct and immediate access to the information (including documents) obtained and used by the Bank, specified by the legislation and this Policy.

1.6. The employees of the Financial Security Division shall have the qualification based on the professional compliance criteria and by the procedure specified by the Authorized Body, meet other criteria, specified by the Authorized Body.

1.7. The employees of the Financial Security Division are hired and dismissed by the Chief Executive Officer of the Bank, upon the consent of the Bank’s Board.

1.8. The Chief Executive Officer of the Bank ensures the implementation of this Policy, approved by the Bank’s Board, as well as its efficient execution.

1.9. The Bank is obliged to ensure the establishment of this Policy and more strict rules for its subsidiaries, branches and representations, located in foreign countries, including Non-compliant countries or territories, than the laws and legal acts of the countries or territories of its subsidiaries, branches and representations. If the laws and other legal act of the countries and territories, where the subsidiaries, branches and representations are located, prohibit or do not provide an opportunity to apply the requirements of this Policy, the Bank shall inform of it the Authorized Body.

UNIT TWO

PROCESS OF COMBATING ML/TF

CHAPTER 2. PREVENTION OF ML/TF, TRANSACTIONS OR BUSINESS RELATIONSHIPS SUBJECT TO REPORTING TO THE AUTHORIZED BODY

2.1. The Bank detects and assesses its possible and available ML/TF risks and it has an efficient management and deterrence policy, control mechanisms and internal legal acts for detected risks.

2.2. The Bank regularly, but not later than on annual basis, reviews its possible and available ML/TF risks.

2.3. The bank detects and assesses the possible and available risks related to the provision of new type

	QUALITY MANAGEMENT SYSTEM	MANUAL 14#6		
	“ACBA-CREDIT AGRICOLE BANK” CJSC POLICY OF FINANCIAL SECURITY	<i>Edition date 11/09/14</i>	<i>Edition 1</i>	<i>Page 6 of 12</i>

of services or the application of the methods of their provision, as well as to the application of new or developing technologies. The risks specified under this clause shall be detected and assessed prior to the provision of the new services or the application of the methods of their provision or the application of new or developing technologies.

2.4. The Bank submits the information on ML/TF, including the information containing secrets, specified by law to the Authorized Body.

2.5. The Bank submits a report to the Authorized Body on suspicious transaction or business relationship and (or) on transactions subject to mandatory reporting.

2.6. The suspicious transaction or business relationship shall be reported irrespective of the size of the amount.

2.7. The transactions subject to mandatory reporting are:

- a) non-cash transactions, the amount of which is equal to or exceeds AMD 20 mln,
- b) cash transactions, the amount of which is equal to or exceeds AMD 5 mln.

2.8. The cases of release from the liability to submit reports on the transactions subject to mandatory reporting are specified by the Authorized Body.

2.9. It is prohibited to the Bank, Bank's employees and representatives to inform the person, regarding whom the report or other information is submitted to the Authorized Body, as well as other people of the fact of provision of the report or other information.

CHAPTER 3. FUNCTIONS OF THE BANK'S MANAGEMENT BODIES AND FINANCIAL SECURITY DEPARTMENT ON COMBATING ML/TF

3.1. The Bank's Board:

- Defines and approves this Policy and the internal legal acts on prevention of ML/TF,
- Approves the annual program of the Financial Security Division and the internal audit on prevention of ML/TF, the reports on their performance, controls the implementation of these programs,
- If required, instructs the Financial Security Division to perform studies, approves the activities directed to the elimination of shortcomings detected during the audit, and controls their execution,
- Discusses and approves the conclusions of the internal audit, as well as by its own specified frequency, but not later than on semi-annual basis – the reports of the Financial Security Division.

3.2. The Chief Executive Officer of the Bank:

- Ensures the complete and efficient application of the legislation and the internal legal acts on prevention of ML/TF and controls it,
- Ensures the proper training of the Bank's employees on prevention of ML/TF,
- Ensures the execution of studies of the Financial Security Division, activities directed to the elimination of the shortcomings detected during the audit.

3.3. The Financial Security Division makes the final decision on the classification of the transaction or business relationship as suspicious, on its suspension, rejection of its execution or termination, freezing the property of persons related to the terrorism, as well as ensures the provision of reports, specified by the Law and this Policy, and the performance of other functions, specified by other internal legal acts.

3.4. The Financial Security Division informs of its final decision on the classification of the transaction or business relationship as suspicious, on its suspension, rejection of its execution or termination, freezing the property of persons related to the terrorism to the Chief Executive Officer of the Bank and to the Board, after the provision of the report on suspicious transaction or business relationship to the Authorized Body, and after the decision on the classification of the transaction or business relationship as suspicious, on its suspension, rejection of its execution or termination, freezing the property of persons related to the terrorism.

3.5. The Financial Security Division regularly, but not later than on semi-annual basis, checks the compliance of the Bank's performed transactions and approved business relationships, the actions of the structural and territorial subdivisions and the employees with the Law, this Policy and the internal legal acts adopted on its basis. The Financial Security Division submits a report on the study results, as well as other issues raised by the Authorized Body, to the Bank's Board.

3.6. The Bank, the Bank's employees (managers) may not be subject to property criminal, administrative or other responsibility for the proper execution of their responsibilities, envisaged by the Law.

	QUALITY MANAGEMENT SYSTEM	MANUAL 14#6		
	“ACBA-CREDIT AGRICOLE BANK” CJSC POLICY OF FINANCIAL SECURITY	<i>Edition date</i> 11/09/14	<i>Edition 1</i>	<i>Page 7 of 12</i>

CHAPTER 4. APPLICATION OF APPROACH BASED ON ML/TF RISKS

4.1. Performing due diligence of the customer in the Bank there is a risk management system implemented, which excludes and assesses the possible or available risks and ensures the initiation of activities equivalent to the risks.

4.2. In case of high risk criterion, the Bank performs customer’s enhanced due diligence, and in case of low risk criterion – customer’s simplified due diligence.

4.3. The simplified due diligence cannot be performed in case of ML/TF high risk criterion or suspicion in transaction or business relationship.

4.4. The Bank performs due diligence also for the available customers, based on the risks related to these customers and their significance.

CHAPTER 5. CUSTOMER DUE DILIGENCE, RELEVANT LIABILITIES

5.1. It is prohibited in the Bank to open, issue, provide or service:

- a) anonymous accounts or accounts in fictitious names,
- b) accounts solely expressed in numbers, letters or other conventional signs,
- c) shares by presenter.

5.2. It is prohibited in the Bank to establish correspondent or other similar relationship with fake (shell) banks.

5.3. The Bank does not establish business relationship with a customer without a face-to-face communication.

5.4. Any business relationship with a customer may be established or an occasional transaction may be concluded only upon the receipt of the identification information (including documents) by the Bank as specified by Clause 5.6 of this Policy and upon checking their veracity. Reporting entities may obtain the identification information specified in this Law and check their veracity also in the course of establishing a business relationship or concluding an occasional transaction or thereafter within a reasonable timeframe, but not later than within 7 days, provided that the risk of money laundering or terrorism financing has been effectively prevented and that this is necessary in order not to impair the normal business relationships.

5.5. The Bank should identify their customers and verify their identity, when:

- a) business relationship is being established,
- b) occasional transaction is being carried out (including affiliated occasional transactions) at a value above 400-fold of the minimal salary,
- c) suspicions arise with regard to the veracity or adequacy of previously obtained customer identification data (including documents),
- d) suspicions arise with regard to the ML/TF.

5.6. When the Bank identifies the customers and verifies their identity on the basis of the reliable and valid documents issued by the state authorized body:

- The information required for natural persons and private entrepreneurs, based on an identification document or another valid official document exceptionally with a photo and issued by a respective authorized state body shall at least include the first and last names of the person, the citizenship, the place of residence (if available), the date and place of birth of the person, the details of the identification document, and for private entrepreneurs also the number of the state registration certificate and the taxpayer identification number, as well as other information stipulated by law. The Bank performs relevant actions also to identify the place of residence of the customer.

- The information required for legal entities based on the state registration document or another official document shall at least include the name, the location, the identification number (number of the state registration certificate and the taxpayer identification number of the legal entity), the first name and the last name of the head of the executive body, and if available the taxpayer identification number, as well as other information stipulated by law and the internal legal acts of the Bank.

- The information required for state bodies or local self-governed bodies shall at least include the full official name and country of the state body or local self-governed body.

5.7. For the establishment of business relationship or an occasional transaction the Bank requires the originals of the documents, required for the identification, which shall be valid, with the last edition and validity.

	QUALITY MANAGEMENT SYSTEM	MANUAL 14#6		
	“ACBA-CREDIT AGRICOLE BANK” CJSC POLICY OF FINANCIAL SECURITY	<i>Edition date 11/09/14</i>	<i>Edition 1</i>	<i>Page 8 of 12</i>

5.8. The Bank identifies if the customer acts on his/her behalf or on behalf of and (or) for the benefit of another person. The Bank:

- Checks the availability of an authorized person, and if available, identifies the authorized person, checks his/her identity, and his/her authorization to act on behalf of the customer;
- Checks the availability of a beneficial owner, and if available, identifies the beneficial owner, checks his/her identity.

5.9. In case of the customer, being the legal entity, in order to identify the beneficial owner of the customer, the Bank collects full information on the authorizations of the participants of that legal entity (with the exception of the reporting issuers, envisaged by the regulating legislation of the securities market) and the management bodies.

5.10. The Bank checks the business description of the customer, as well as checks the purpose of the business relationship and the envisaged nature.

5.11. If the customer is a foreign legal entity or a foreign natural person or an entity without the status of a legal person under foreign legislation, then the Bank shall be obligated to identify and document also the center of these persons' vital interests.

5.12. The Bank shall take adequate measures to identify the politically exposed persons or their family members (father, mother, husband, wife, grandmother, grandfather, sister, brother, children, parents of husband/wife) or persons affiliated with them, by applying special databases and software.

5.13. The data obtained as a result of customer identification and verification by other financial institution or non-financial institution or a person may serve as a basis for the Bank in the course of customer identification and verification only given the conditions below:

- 1) the Bank bears the final responsibility for the due diligence of the customer,
- 2) the Bank receives the information, specified under clauses 5.4-5.6 and 5.8-5.10 of this Policy directly from other financial institution or non-financial institution or a person,
- 3) the Bank takes sufficient measures to make sure that other financial institution or non-financial institution or a person:
 - a) is authorized and can immediately upon request, submit the information obtained as a result of the customer's due diligence, including the copies of the documents,
 - b) from the viewpoint of combating ML/TF, is subject to proper regulation and control, as well as has efficient procedures for the due diligence of the customer and processing of information, envisaged by the Law and legal acts, adopted on its basis,
 - c) is not located or residing in the Non-compliant countries or territories or is not from the Non-compliant country or territory.

5.14. The Bank shall conduct ongoing customer due diligent throughout the course of a business relationship. In the course of customer due diligence, the Bank shall conduct monitoring of the transactions with the customer in order to ensure veracity of the information on the customer, his/her business and risk profile and, where necessary, of the source of his/her income.

5.15. At a frequency determined by their own, but not later than on annual basis, the Bank should update the data obtained due to customer identification (including enhanced or simplified due diligence) in the business relationship to ensure their validity and correspondence.

5.16. During the correspondent or other similar relationship with the foreign financial institutions, besides the requirements of the customer's due diligence, the Bank:

- a) collects sufficient information to fully detect the business nature of the correspondent institution, and based on the publicly available and other reliable sources, assesses the business reputation of the correspondent institution and its quality control, including the fact whether the correspondent institution has been or is involved in the criminal prosecution or other proceedings related to combating ML/TF,
- b) assesses the procedures on combating ML/TF, implemented by the correspondent institution, to make sure that they are sufficient and effective,
- c) establishes correspondent or other similar relationship upon the approval of the Senior Management,
- d) documents the relevant liabilities on combating ML/TF of each of the correspondent institutions, if they are not clearly known.

5.17. During the correspondent or other similar relationship, the Bank does not open transit accounts.

5.18. When carrying out wire transfers, the following information shall be requested and maintained by

	QUALITY MANAGEMENT SYSTEM	MANUAL 14#6		
	“ACBA-CREDIT AGRICOLE BANK” CJSC POLICY OF FINANCIAL SECURITY	<i>Edition date 11/09/14</i>	<i>Edition 1</i>	<i>Page 9 of 12</i>

the Bank:

- a) name and surname of the originator and the addressee,
- b) account numbers of the originator and the addressee (in its absence, the unique reference number accompanying the transfer),
- c) details of the identification document of the natural person, or the identification number (state registration number, residence number, etc.) of the legal entity.

5.19. The information, specified under Clause 5.18 of this Policy is also included in the payment order accompanying the transfer.

5.20. The obligations stipulated by Clause 5.18 of this Policy shall not apply to the transactions carried out through the use of credit, debit or advance cards, provided that all accompanying messages (accompanying notes) of the transaction include information about the numbers of such cards. This exclusion refers to the cases, when the transaction relates to the encashment, payment for goods or services through ATMs, as well as to the cases, when the credit, debit or advance cards are used for transfers via any payment systems.

5.21. When the Bank is an intermediary or the recipient of a wire transfer, applying the approach based on the risks, the Bank detects and takes the required measures (including rejection or suspension of the transaction) towards the transfers, which do not contain the information, specified by Clause 5.18 of this Policy. In case of wire transfers, which do not include the information, specified by Clause 5.18 of this Policy, the Bank considers the issue of termination of correspondent or other similar relationship with the financial institution.

CHAPTER 6. MAINTAINING RECORDS

6.1. The Bank may collect and maintain the information (including documents), specified by the Law and this Policy, either in paper form or electronically.

6.2. The Bank maintains the information (including documents), specified by the Law and this Policy, including the information (documents), obtained during the due diligence of the customer, irrespective of the fact of continuation or termination of the transaction or business relationship.

6.3. The Bank maintains the information (including documents), specified by the Law and this Policy, including the information (documents), obtained during the due diligence of the customer, for at least 5 years following the completion of the business relationship or transaction, and if prescribed by law or internal legal acts of the Bank – for a longer period.

6.4. The Bank collects and maintains the information (including documents), specified by the Law and this Policy, including the information (documents), obtained during the due diligence of the customer, so that it will be sufficient for provision of comprehensive information about transactions (business relationships) requested by the Authorized Body or, in cases prescribed by law, by criminal investigation authorities.

6.5. The Bank ensures the availability of the information (including documents), specified by the Law and this Policy, including the information (documents), obtained during the due diligence of the customer, in due terms and by the procedure, established by the law, for the authorized controlling and criminal investigation authorities, as well as for auditors.

CHAPTER 7. RECOGNITION OF A TRANSACTION OR BUSINESS RELATIONSHIP AS SUSPICIOUS

7.1. In case of disclosing the grounds and criteria for suspicious transactions or business relationships, the given transaction or business relationship, including the attempted ones, shall be recognized as suspicious by the Bank, and a respective report shall be immediately filed to the Authorized Body, if it is suspected or there are sufficient grounds to suspect that the business relationship or transaction involves funds or other assets, which are linked to, have been used or intended for use by terrorist organizations or individual terrorists or sponsors of terrorists for the purpose of terrorism.

7.2. The ban considers the issue of recognition a transaction or business relationship as suspicious and submission of a report on suspicious transaction or business relationship to the Authorized Body, if the situation observed fully or partially corresponds to the criteria or typology of suspicious transaction or business relationship, or it becomes evident for the Bank that the suspicion about such transaction or

	QUALITY MANAGEMENT SYSTEM	MANUAL 14#6		
	“ACBA-CREDIT AGRICOLE BANK” CJSC POLICY OF FINANCIAL SECURITY	<i>Edition date 11/09/14</i>	<i>Edition 1</i>	<i>Page 10 of 12</i>

business relationship does not derive from the grounds and criteria for suspicious transactions or business relationship, but the logic and flows (dynamics) of its execution or other circumstances give the grounds to assume that it is being carried out for money laundering and terrorism financing purposes. In cases specified herein, if the transaction or business relationship is not qualified as suspicious and a report on suspicious transaction or business relationship is not filed to the Authorized Body, the grounds for not qualifying the transaction or business relationship as suspicious, conclusions, the process of analysis and the results shall be documented and maintained by the Bank by the procedure and terms, specified by law.

CHAPTER 8. SUSPENSION, REJECTION OF SUSPICIOUS BUSINESS RELATIONSHIPS OR TRANSACTIONS AND FREEZING OF PROCEEDS LINKED TO TERRORISM

8.1. The Bank shall be entitled to suspend a business relationship or transaction for a period of up to 5 days, if there are any suspicions of money laundering, and shall be obligated to suspend for 5 days the business relationship or transaction in case of such an instruction by the Authorized Body, promptly filing a report on the suspicious transaction (business relationship) to the Authorized Body.

8.2. A business relationship or transaction may be suspended for a period of up to 5 days upon the decision of the Authorized Body. The Bank shall promptly enforce the decision of the Authorized Body on suspending a transaction or business relationship upon its receipt.

8.3. Within 5 days after receiving the notification from the Bank about suspension of a transaction or business relationship, or after suspension of a transaction or business relationship by the Authorized Body, the Authorized Body shall decide on sending a statement to criminal investigation authorities on prolonging the suspension for 5 days (in exceptional cases, for 10 days) in order to determine the grounds for sending a statement to criminal investigation authorities, or on revoking the decision on suspension. In case of failure to provide the decision of the Authorized Body to the Bank within the timeframe specified herein, the decision on suspension shall be recognized as revoked.

8.4. The decision of the Bank or the Authorized Body on suspending a business relationship or transaction may be revoked prior to the completion of the suspension term only by the Authorized Body upon its own initiative or upon the request of the Bank, if it has been determined that the suspicion of money laundering or terrorism financing is unjustified.

8.5. The Bank shall be obligated to reject carrying out a business relationship or transaction, that is to refrain from endorsing or carrying out a business relationship or from concluding a transaction, or to terminate execution of a business relationship or transaction based on the decision of the Authorized Body or if they are unable to perform customer identification as a result of the actions undertaken pursuant to clauses 5.4-5.10 of this Policy, and it shall consider the issue of qualifying it as suspicious in accordance with this Policy.

8.6. In cases when on the basis of the second sentence of Clause 5.4 of this Policy, after the establishment of a business relationship, it is not possible to carry out the liabilities envisaged by clauses 5.4-5.10, or in case of receipt of an instruction by the Authorized Body to terminate execution of a business relationship or transaction, the Bank shall terminate the business relationship or transaction and consider the issue of qualifying it as suspicious in accordance with this Policy.

8.7. The Bank rejects any request for transfer of an amount at a value above 400-fold of the minimal salary, if the information, specified by Clause 5.18 of this Policy is absent, as well as it rejects any request for transfer of an amount at a value below 400-fold of the minimal salary, if the information, specified by subclauses “a” and “b” of Clause 5.18 of this Policy is absent, and it shall consider the issue of qualifying it as suspicious in accordance with this Policy.

8.8. With the view of adhering to the resolutions of the UN Security Council, the Authorized Body shall release the lists of the persons linked to terrorism and ensure immediate freezing of funds of the persons included in such lists, as well as of other persons linked to terrorism financing, without prior notification of the customers.

8.9. The Bank is obliged to inform the Authorized Body of any information on persons corresponding to the definition of persons linked to terrorism.

8.10. In case of freezing the property of persons linked to terrorism, the Bank shall immediately recognize the transaction or business relationship as suspicious and file a relevant report on suspicious transaction or business relationship.

	QUALITY MANAGEMENT SYSTEM	MANUAL 14#6		
	“ACBA-CREDIT AGRICOLE BANK” CJSC POLICY OF FINANCIAL SECURITY	<i>Edition date 11/09/14</i>	<i>Edition 1</i>	<i>Page 11 of 12</i>

UNIT THREE

PROCESS OF MAINTENANCE OF INTERNATIONAL SANCTIONS

CHAPTER 9. SCOPE OF MAINTENANCE OF INTERNATIONAL SANCTIONS

9.1. The Bank initiates the relevant activities of the requirements (in particular, applied by the UNO, European Union, France and the USA) of maintenance of international sanctions to avoid the reputation risk.

9.2. The Bank maintains the following types of international sanctions:

- Embargoes, applied to countries,
- Embargoes, applied to product types and (or) business sectors of countries or territories,
- Embargoes, applied to persons,
- Requirements of freezing property.

CHAPTER 10. REQUIREMENTS TO MAINTENANCE OF INTERNATIONAL SANCTIONS

10.1. With its internal legal acts, the Bank specifies the approaches and scope of limitations applied by the Bank regarding the embargoes to the countries, product types and (or) business sectors of countries and territories.

10.2. The Bank performs audit of customers and transaction data by the list of persons under international sanctions.

10.3. The following lists of persons under international sanctions are applied by the Bank:

- Lists of the UN Security Council,
- Lists, specified by the European Union and France,
- OFAC lists, specified by the US Department of the Treasury state body,
- List, specified by the Bank.

10.4. The Bank uses special software for audit by the lists of persons under international sanctions.

10.5. The Bank tracks the amendments in the lists of persons under international sanctions and duly updates them.

10.6. The services of the persons under international sanctions and their transactions are performed, taking into consideration the requirements of the international sanctions.

10.7. The Bank maintains the information, collected within the framework of the international sanctions, in accordance with the rules, specified by Unit 6 of this Policy.

UNIT FOUR

PROCESS OF MAINTENANCE OF FATCA REQUIREMENTS

CHAPTER 11. SCOPE OF MAINTENANCE OF FATCA REQUIREMENTS

11.1. Implementing the FATCA process in the Bank, the latter may use the services of an external consulting organization.

11.2. The Bank has signed a cooperation agreement with the USA Internal Revenue Service and has received the relevant identification number (GIIN).

CHAPTER 12. REQUIREMENTS TO MAINTENANCE OF FATCA REQUIREMENTS

12.1. With its internal legal acts the Bank specifies the approaches to the application of the FATCA requirements.

12.2. The information on customers required by FATCA is collected in accordance with the approaches and scope of “Know Your Customer” principle.

12.3. The Bank maintains the information, collected within the scope of FATCA requirements, according

	QUALITY MANAGEMENT SYSTEM	MANUAL 14#6		
	“ACBA-CREDIT AGRICOLE BANK” CJSC POLICY OF FINANCIAL SECURITY	<i>Edition date 11/09/14</i>	<i>Edition 1</i>	<i>Page 12 of 12</i>

to the rules of Unit 6 of this Policy.

UNIT FIVE

CONCLUDING AND TRANSITIONAL PROVISIONS

CHAPTER 13. CONCLUDING PROVISIONS

13.1. In cases and frequency, specified by the Authorized Body, the Bank performs internal audit to audit the proper execution of liabilities and functions, stipulated by the Law and this Policy.

13.2. The conclusions of the internal audit (including those of the ML/TF Prevention Division on report on the implementation of the annual program of the internal audit) shall be properly submitted to the Authorized Body within one week upon their approval by the Bank's Board.

13.3. By the procedure, established by the Authorized Body, the Bank invites an external audit upon the request of the Authorized Body or by its own initiative, to audit the level of implementation and efficiency of the requirements of the legislation on combating ML/TF, this Policy and other requirements.

13.4. The Bank regularly organizes trainings on financial security for the Bank's Board, executive body, Financial Security Division, staff performing customer service and internal audit functions, as well as for other employees, working in the financial security sector.

13.5. The Bank organizes trainings on financial security for the new employees of the Bank within three months upon employment.

13.6. The Bank registers and maintains the training materials, data on training participants and documents evidencing the participation for at least 5 years.

CHAPTER 14. TRANSITIONAL PROVISIONS

14.1. The provisions of this document, the application of which envisages the adoption of the relevant internal legal acts by the authorized management bodies of the Bank, shall enter into force from the validity date of the given acts.

14.2. In case of amendments and (or) additions made to the valid legislation in the future, the Bank shall be guided by those amendments and (or) additions until the adjustment of this Policy to the requirements of the new legislation.

14.3. In case of approval of this Policy, as well as amendments and (or) additions made to it, the Bank shall submit the copy of the Policy to the Central Bank of the Republic of Armenia within one week.

14.4. All employees of the Bank shall get acquainted with this document on a mandatory basis.

14.5. This document shall enter into force from 25 November 2014.