



COMMITTEE OF EXPERTS ON THE
EVALUATION OF ANTI-MONEY
LAUNDERING MEASURES AND THE
FINANCING OF TERRORISM
(MONEYVAL)

MONEYVAL(2010)15 ANN

Armenia

Progress report - *Annexes*¹

28 September 2010

¹ First 3rd Round Written Progress Report Submitted to MONEYVAL

Armenia is a member of MONEYVAL. This progress report was adopted at MONEYVAL's 33rd Plenary meeting (Strasbourg, 27 September – 1 October 2010). For further information on the examination and adoption of this report, please refer to the Meeting Report (ref. MONEYVAL(2010)32) at <http://www.coe.int/moneyval>

© [2010] European Committee on Crime Problems (CDPC)/ Committee of experts on the evaluation of anti-money laundering measures and the financing of terrorism (MONEYVAL)

All rights reserved. Reproduction is authorised, provided the source is acknowledged, save where otherwise stated. For any use for commercial purposes, no part of this publication may be translated, reproduced or transmitted, in any form or by any means, electronic (CD-Rom, Internet, etc) or mechanical, including photocopying, recording or any information storage or retrieval system without prior permission in writing from the MONEYVAL Secretariat, Directorate General of Human Rights and Legal Affairs, Council of Europe (F-67075 Strasbourg or dghl.moneyval@coe.int).

Table of Contents

ANNEX 1 - REPUBLIC OF ARMENIA DRAFT LAW ON MAKING A CHANGE IN THE REPUBLIC OF ARMENIA LAW ON COMBATING MONEY LAUNDERING AND TERRORISM FINANCING ®	5
ANNEX 2 - REPUBLIC OF ARMENIA DRAFT LAW ON MAKING CHANGES AND AMENDMENTS IN THE REPUBLIC OF ARMENIA CRIMINAL CODE ®	5
ANNEX 3 - REPUBLIC OF ARMENIA DRAFT LAW ON MAKING A CHANGE AND AMENDMENTS IN THE REPUBLIC OF ARMENIA CRIMINAL PROCEDURE CODE ®	5
ANNEX 4 - REPUBLIC OF ARMENIA DRAFT LAW ON MAKING A CHANGE IN THE REPUBLIC OF ARMENIA ADMINISTRATIVE VIOLATIONS CODE ®	5
ANNEX 5 - REPUBLIC OF ARMENIA DRAFT LAW ON MAKING A CHANGE AND AMENDMENTS IN THE REPUBLIC OF ARMENIA CUSTOMS CODE ®	5
ANNEX 6 - REPUBLIC OF ARMENIA DRAFT LAW ON MAKING A CHANGE AND AMENDMENTS IN THE REPUBLIC OF ARMENIA LAW ON BANK SECRECY ®	5
ANNEX 7 - REPUBLIC OF ARMENIA DRAFT LAW ON MAKING A CHANGE AND AN AMENDMENT IN THE REPUBLIC OF ARMENIA LAW ON INSURANCE AND INSURANCE ACTIVITIES ®	5
ANNEX 8 - REPUBLIC OF ARMENIA DRAFT LAW ON MAKING AMENDMENTS IN THE REPUBLIC OF ARMENIA LAW ON LICENSING ®	6
ANNEX 9 - REPUBLIC OF ARMENIA DRAFT LAW ON MAKING AN AMENDMENT IN THE REPUBLIC OF ARMENIA LAW ON ORGANIZING AND CONDUCTING INSPECTIONS IN THE REPUBLIC OF ARMENIA ®	6
ANNEX 10 - REPUBLIC OF ARMENIA DRAFT LAW ON MAKING AN AMENDMENT IN THE REPUBLIC OF ARMENIA LAW ON ACCOUNTING ®	6
ANNEX 11 - REPUBLIC OF ARMENIA DRAFT LAW ON MAKING A CHANGE AND AMENDMENTS IN THE REPUBLIC OF ARMENIA LAW ON AUDITING ACTIVITIES ®	6
ANNEX 12 - REPUBLIC OF ARMENIA DRAFT LAW ON MAKING AMENDMENTS IN THE REPUBLIC OF ARMENIA LAW ON ADVOCACY ®	6
ANNEX 13 - REPUBLIC OF ARMENIA DRAFT LAW ON MAKING A CHANGE AND AMENDMENTS IN THE REPUBLIC OF ARMENIA LAW ON THE NOTARIAL SYSTEM ®	6
ANNEX 14 - REPUBLIC OF ARMENIA DRAFT LAW ON MAKING AN AMENDMENT IN THE REPUBLIC OF ARMENIA LAW ON DECLARATION OF PROPERTY AND INCOME OF NATURAL PERSONS ®	6
ANNEX 15 - REPUBLIC OF ARMENIA DRAFT LAW ON MAKING CHANGES AND AMENDMENTS IN THE REPUBLIC OF ARMENIA LAW ON GAMES OF CHANCE AND CASINO ®	7
ANNEX 16 - REPUBLIC OF ARMENIA DRAFT LAW ON MAKING CHANGES AND AMENDMENTS IN THE REPUBLIC OF ARMENIA LAW ON LOTTERIES ®	7
ANNEX 17 - REPUBLIC OF ARMENIA DRAFT LAW ON MAKING AN AMENDMENT IN THE REPUBLIC OF ARMENIA LAW ON STATE REGISTRATION OF PROPERTY RIGHTS ®	7
ANNEX 18 - REPUBLIC OF ARMENIA LAW ON POSTAL COMMUNICATION	7

ANNEX 19 - 2010-2013 NATIONAL STRATEGY FOR COMBATING MONEY LAUNDERING AND TERRORISM FINANCING	8
ANNEX 20 - MANUAL ON CONDUCTING A STRATEGIC ANALYSIS OF MONEY LAUNDERING AND TERRORISM FINANCING RISK IN THE REPUBLIC OF ARMENIA ®.....	16
ANNEX 21 - SUMMARY OF CONDUCTING A STRATEGIC ANALYSIS OF MONEY LAUNDERING AND TERRORISM FINANCING RISK IN THE REPUBLIC OF ARMENIA.....	17
ANNEX 22 – EXTRACT FROM PROTOCOL N 6 OF OCTOBER 21, 2009 ON ENSURING THE IMPLEMENTATION OF DECISIONS APPROVED ON OCTOBER 21, 2009 AT THE MEETING OF THE BOARD OF THE PROSECUTION OFFICE OF THE REPUBLIC OF ARMENIA®.....	27
ANNEX 23 - GUIDANCE FOR SOLE PRACTITIONER ACCOUNTANTS, ACCOUNTING FIRMS AND SOLE PRACTITIONER AUDITORS, AUDITING FIRMS ON MINIMAL REQUIREMENTS FOR ASSESSING AND PREVENTING MONEY LAUNDERING AND TERRORISM FINANCING RISKS	28
ANNEX 24 - GUIDANCE for ENTITIES ENGAGED IN REALTOR ACTIVITIES ON MINIMAL REQUIREMENTS FOR ASSESSING AND PREVENTING MONEY LAUNDERING AND TERRORISM FINANCING RISKS.....	40
ANNEX 25 - GUIDANCE FOR ENTITIES ORGANIZING GAMES OF ChANCE AND LOTTERIES AND CASINOS, INCLUDING ENTITIES ORGANISING ONLINE GAMES OF CHANCE, ON MINIMAL REQUIREMENTS FOR ASSESSING AND PREVENTING MONEY LAUNDERING AND TERRORISM FINANCING RISKS.....	51
ANNEX 26 - GUIDANCE for ATTORNEYS, SOLE PRACTITIONER LAWYERS AND FIRMS PROVIDING LEGAL SERVICES ON MINIMAL REQUIREMENTS FOR ASSESSING AND PREVENTING MONEY LAUNDERING AND TERRORISM FINANCING RISKS.....	62
ANNEX 27 – EXTRACT FROM THE DECISION OF THE CHAIRMAN OF THE REPUBLIC OF ARMENIA CENTRAL BANK No 1-1315L OF OCTOBER 19, 2009 (ON ON-SITE INSPECTIONS IN BANKS).....	74
ANNEX 28 – DECISION OF THE CHAIRMAN OF THE REPUBLIC OF ARMENIA CENTRAL BANK No 1/1178L of NOVEMBER 28, 2008 (ON ON-SITE INSPECTIONS IN CREDIT ORGANIZATIONS).....	84
ANNEX 29 – EXTRACT FROM THE DECISION OF THE ChAIRMAN OF THE REPUBLIC OF ARMENIA CENTRAL BANK No 1-1454A of NOVEMBER 25, 2009 (ON ON-SITE INSPECTIONS IN INSURANCE COMPANIES).....	85
ANNEX 30 - EXTRACT FROM THE DECISION OF THE CHAIRMAN OF THE REPUBLIC OF ARMENIA CENTRAL BANK No 1/139A of FEBRUARY 24, 2010 (ON ON-SITE INSPECTIONS IN INVESTMENT COMPANIES).....	94
ANNEX 31 - CENTRAL BANK OF ARMENIA BOARD DRAFT DECISION ON MAKING AN AMENDMENT TO THE CENTRAL BANK OF ARMENIA BOARD DECISION N 386-N, DATED JULY 29, 2005 ®	102

ANNEX 1 - REPUBLIC OF ARMENIA DRAFT LAW ON MAKING A CHANGE IN THE REPUBLIC OF ARMENIA LAW ON COMBATING MONEY LAUNDERING AND TERRORISM FINANCING ®

Restricted

ANNEX 2 - REPUBLIC OF ARMENIA DRAFT LAW ON MAKING CHANGES AND AMENDMENTS IN THE REPUBLIC OF ARMENIA CRIMINAL CODE ®

Restricted

ANNEX 3 - REPUBLIC OF ARMENIA DRAFT LAW ON MAKING A CHANGE AND AMENDMENTS IN THE REPUBLIC OF ARMENIA CRIMINAL PROCEDURE CODE ®

Restricted

ANNEX 4 - REPUBLIC OF ARMENIA DRAFT LAW ON MAKING A CHANGE IN THE REPUBLIC OF ARMENIA ADMINISTRATIVE VIOLATIONS CODE ®

Restricted

ANNEX 5 - REPUBLIC OF ARMENIA DRAFT LAW ON MAKING A CHANGE AND AMENDMENTS IN THE REPUBLIC OF ARMENIA CUSTOMS CODE ®

Restricted

ANNEX 6 - REPUBLIC OF ARMENIA DRAFT LAW ON MAKING A CHANGE AND AMENDMENTS IN THE REPUBLIC OF ARMENIA LAW ON BANK SECRECY ®

Restricted

ANNEX 7 - REPUBLIC OF ARMENIA DRAFT LAW ON MAKING A CHANGE AND AN AMENDMENT IN THE REPUBLIC OF ARMENIA LAW ON INSURANCE AND INSURANCE ACTIVITIES ®

Restricted

ANNEX 8 - REPUBLIC OF ARMENIA DRAFT LAW ON MAKING AMENDMENTS IN THE REPUBLIC OF ARMENIA LAW ON LICENSING ®

Restricted

ANNEX 9 - REPUBLIC OF ARMENIA DRAFT LAW ON MAKING AN AMENDMENT IN THE REPUBLIC OF ARMENIA LAW ON ORGANIZING AND CONDUCTING INSPECTIONS IN THE REPUBLIC OF ARMENIA ®

Restricted

ANNEX 10 - REPUBLIC OF ARMENIA DRAFT LAW ON MAKING AN AMENDMENT IN THE REPUBLIC OF ARMENIA LAW ON ACCOUNTING ®

Restricted

ANNEX 11 - REPUBLIC OF ARMENIA DRAFT LAW ON MAKING A CHANGE AND AMENDMENTS IN THE REPUBLIC OF ARMENIA LAW ON AUDITING ACTIVITIES ®

Restricted

ANNEX 12 - REPUBLIC OF ARMENIA DRAFT LAW ON MAKING AMENDMENTS IN THE REPUBLIC OF ARMENIA LAW ON ADVOCACY ®

Restricted

ANNEX 13 - REPUBLIC OF ARMENIA DRAFT LAW ON MAKING A CHANGE AND AMENDMENTS IN THE REPUBLIC OF ARMENIA LAW ON THE NOTARIAL SYSTEM ®

Restricted

ANNEX 14 - REPUBLIC OF ARMENIA DRAFT LAW ON MAKING AN AMENDMENT IN THE REPUBLIC OF ARMENIA LAW ON DECLARATION OF PROPERTY AND INCOME OF NATURAL PERSONS ®

Restricted

ANNEX 15 - REPUBLIC OF ARMENIA DRAFT LAW ON MAKING CHANGES AND AMENDMENTS IN THE REPUBLIC OF ARMENIA LAW ON GAMES OF CHANCE AND CASINO ®

Restricted

ANNEX 16 - REPUBLIC OF ARMENIA DRAFT LAW ON MAKING CHANGES AND AMENDMENTS IN THE REPUBLIC OF ARMENIA LAW ON LOTTERIES ®

Restricted

ANNEX 17 - REPUBLIC OF ARMENIA DRAFT LAW ON MAKING AN AMENDMENT IN THE REPUBLIC OF ARMENIA LAW ON STATE REGISTRATION OF PROPERTY RIGHTS ®

Restricted

ANNEX 18 - REPUBLIC OF ARMENIA LAW ON POSTAL COMMUNICATION

Excerpt

Adopted on December 14, 2004

Article 20. The responsibility of the users of postal service and restrictions

It is prohibited to deliver the following items by mail:

- a)(...)
- b)(...)
- c)(...)
- d) bank-notes of the Republic of Armenia and foreign currency (except for the deliveries of the Central Bank of Armenia and other banks);
- e) (...)
- f) (...).

January 15, 2005

HO-46-N

ANNEX 19 - 2010-2013 NATIONAL STRATEGY FOR COMBATING MONEY LAUNDERING AND TERRORISM FINANCING

Approved on March 26, 2010 at the meeting of the
Interagency Commission on the Fight against Counterfeiting of Money,
Fraud in Plastic Cards and Other Payment Instruments,
Money Laundering and Terrorism Financing

Vision

Develop capacities for money laundering and terrorism financing (ML/FT) prevention and criminal prosecution, ensure that ML/FT offences are subject to punishments and promote the formation of social intolerance towards ML/FT offences.

Qualitative changes

Moving to second generation AML/CFT reformations with features as follows:

1. Shifting from basic AML/CFT legislation towards a legal framework that largely complies with FATF standards and comprises several levels of legislative hierarchy.
2. Setting forth equal AML/CFT requirements for all reporting entities (financial institutions and designated non-financial businesses and professions) and ensuring the implementation thereof.
3. Shifting from the standardized implementation of AML/CFT mechanisms towards the application of risk-based approach mechanisms.
4. Adopting an efficient, operative and unified work regime based on the specialization of ML/FT criminal prosecution and judicial proceeding functions and the present practices.

Values

For the purpose of implementing this strategy, all the participants of the AML/CFT system should strictly follow and commit to the following values:

1. Professionalism
2. Justice
3. Cooperation
4. Mutual respect
5. Trust
6. Required confidentiality in current tasks, publicity of projects and results
7. Initiation

Strategic directions and their results

No	Strategic directions /Predetermined measures	Expected results	Agencies and institutions involved	Additional funding sources required	Timeframe
1	Coordinated national policy in the field of AML/CFT				
1.1	Discussing all important strategic issues and measures and coordinating positions within the scope of the AML/CFT Interagency Commission (hereinafter: Interagency Commission).	Presence of coordinated positions on strategic issues and measures.	Member agencies and institutions of the Interagency Commission	Not required	2010-2013
1.2	Establishing mechanisms for periodic reporting to the Interagency Commission on the results of activities of agencies and authorities in the field of AML/CFT.	Accessible information on the activities conducted in the field of AML/CFT, realization of the performance report.	Secretariat of the Interagency Commission	Not required	2010-2013
2	Developing a legal framework that complies with international AML/CFT standards				
2.1	Improving the AML/CFT legal framework of the RA based on the recommendations presented by the Council of Europe's MONEYVAL Committee (MONEYVAL) and the International Monetary Fund in the third round assessment report of the AML/CFT system	- Adoption of legal acts that largely comply with FATF standards, take into consideration the characteristics of different spheres and comprise several levels of legislative hierarchy, publication of methodical clarifications and guidance on	Member agencies and institutions of the Interagency Commission	Not required	2010-2011

	of the Republic of Armenia.	the implementation thereof, - Proclamation of compliance with recommendations on AML/CFT legal framework in the progress report of the Republic of Armenia that is subject to submission to MONEYVAL.			
2.2	Preparing and moving to the MONEYVAL fourth round assessment.	- Preparation of materials required for the assessment, undertaking all other administrative measures in a coordinated manner, - Proclamation of progress in the AML/CFT system under the fourth round assessment report as in contrast to the third round assessment report.	Member agencies and institutions of the Interagency Commission	Not required	2012-2013
3	Developing capacities for the Financial Monitoring Center of the Republic of Armenia (FMC) as a financial intelligence unit				
3.1	Purchasing/developing analytical software systems by the FMC and implementation thereof in analyses processes.	Increase in value of the FMC analyses for criminal prosecution purposes.	FMC	Central Bank budget, funding from international donors	2010-2013
3.2	Designing and developing electronic documentation flow and task management software systems by the FMC.	Optimization of the FMC internal processes.	FMC	Funding from international donors	2010-2011
3.3	Conducting strategic analyses	Periodic summarization and	FMC	Not required	2010-2013

	on ML/FT trends and schemes by the FMC by means of implementing and developing international typologies.	publication of analyses on ML/FT trends and schemes.			
3.4	Organizing practical training courses for the FMC employees at foreign financial intelligence units.	Implementation of foreign financial intelligence units' experiences into the works of the FMC.	FMC	Central Bank budget, funding from international donors	2010-2013
4	Developing capacities for operative intelligence and criminal prosecution of ML/FT				
4.1	Formation of units inside criminal prosecution bodies with specialization in operative intelligence and criminal prosecution of ML/FT.	Improvement of efficiency in operative intelligence and criminal prosecution of ML/FT.	Prosecution Office of the RA, National Security Service of the RA, Police of the RA, State Revenue Committee adjunct to the Government of the RA	State budget of the RA, funding from international donors	2010-2013
4.2	Developing professional skills for operative intelligence, criminal prosecution and judicial proceedings of ML/FT in criminal prosecution bodies and courts by means of trainings and workshops.	Increase in efficiency of the ML/FT punishment function.	Prosecution Office of the RA, National Security Service of the RA, Police of the RA, State Revenue Committee adjunct to the Government of the RA, Court Department of the RA	State budget of the RA, funding from international donors	2010-2013
5	Developing capacities for supervisory authorities in the field of AML/CFT				
5.1	Developing capacities for verifying compliance with AML/CFT requirements within the process of supervision of financial and non-financial	Ensured compliance of financial and non-financial institutions' operations with AML/CFT requirements.	Central Bank of the RA, Ministry of Justice of the RA, Ministry of Finance of the RA, State Committee of the Real	State budget of the RA, Central Bank budget, funding from international donors	2010-2013

	institutions by means of trainings, workshops, provided guidance and other methods.		Estate Cadastre adjunct to the Government of the RA		
6	Formation of an integrated information portal for AML/CFT				
6.1	- Integrating the databases of authorized agencies of the RA (in particular, the Passport and Information Center of the Police of the RA, database of the State Revenue Committee adjunct to the Government of the RA) into the database of the FMC, - Ensuring direct access of the FMC to this database and indirect access (by means of requests) for the other authorized agencies.	Formation of largest possible information resource for financial analyses of ML/FT cases and improvement in complexity and accuracy of such analyses.	Member agencies and institutions of the Interagency Commission	Central Bank budget, funding from international donors	2010-2013
7	Developing capacities for reporting entities in the field of AML/CFT				
7.1	Developing professional skills for employees of reporting entities performing the function of the internal monitoring unit by means of trainings, workshops, qualifications and provided guidance.	Presence of efficient AML/CFT mechanisms with reporting entities.	FMC, Ministry of Justice of the RA, Ministry of Finance of the RA, State Committee of the Real Estate Cadastre adjunct to the Government of the RA	Central Bank budget, funding from international donors	2010-2013
7.2	Ensuring compliance of AML/CFT internal legal acts of reporting entities with	Description of AML/CFT mechanisms with financial institutions, ensured	FMC	Not required	2010-2013

	AML/CFT national legislation and the implementation thereof by means of periodically reviewing the acts and verifying the implementation efficiency in the course of conducting supervision.	implementation thereof.			
7.3	Promoting the implementation of ML/FT risk-based approach with reporting entities.	Assessment of internal ML/FT risks by financial institutions based on legal acts and guidance and presence of efficient prevention measures.	FMC, Ministry of Justice of the RA, Ministry of Finance of the RA, State Committee of the Real Estate Cadastre adjunct to the Government of the RA, self-regulated organizations	Funding from international donors	2010-2013
7.4	Ensuring appropriate implementation of AML/CFT requirements by non-financial institutions by means of trainings, workshops, qualifications and provided guidance.	Reduction of non-financial institutions' involvement risk in ML/FT.	Central Bank of the RA, Ministry of Justice of the RA, Ministry of Finance of the RA, State Committee of the Real Estate Cadastre adjunct to the Government of the RA, self-regulated organizations of non-financial institutions	State budget of the RA, Central Bank budget, funding from international donors	2010-2013
8	Building intrastate cooperation in the field of AML/CFT				
8.1	Implementing efficient mechanisms for bilateral cooperation between authorized	Effective integration of intrastate institutional and functional mechanisms in the	Member agencies and institutions of the Interagency Commission	Not required	2010-2013

	agencies and institutions by means of mutual advisory, formation of shared working groups, signing of agreements and other methods.	field of AML/CFT.			
9	Building international cooperation in the field of AML/CFT				
9.1	Active involvement in the works of MONEYVAL and the Eurasian Group on combating money laundering and financing of terrorism.	Demonstration of the AML/CFT system of the Republic of Armenia to the international professional society by means of involvement in the works of FATF-style regional bodies as mentioned.	Member agencies and institutions of the Interagency Commission	State budget of the RA, Central Bank budget, funding from international donors	2010-2013
9.2	Enhancing cooperation with foreign financial intelligence units within the framework of the Egmont Group by means of sponsoring candidate FIUs, signing MoU-s with member FIUs, effective exchange of information as well as active involvement in the initiatives emerged within the framework of the Egmont Group.	Strong international status for the FMC as a financial intelligence unit and improved professional rating.	FMC	Central Bank budget	2010-2013
9.3	Conducting activities with other international structures in the field of AML/CFT by means of involvement in the works	Demonstration of the AML/CFT system of the Republic of Armenia in other international structures,	Member agencies and institutions of the Interagency Commission	Funding from international donors	2010-2013

	thereof, receiving technical assistance and organization of training courses through these structures.	utilization of international resources for the development of this system.			
9.4	Enhancing bilateral relationships between law enforcement and supervisory authorities in the field of AML/CFT and foreign agencies by means of signing MoU-s, mutual interaction, exchange of information and other methods.	Effective cooperation between law enforcement and supervisory authorities in the field of AML/CFT and analogous foreign agencies.	Member agencies and institutions of the Interagency Commission	State budget of the RA	2010-2013

**ANNEX 20 - MANUAL ON CONDUCTING A STRATEGIC
ANALYSIS OF MONEY LAUNDERING AND TERRORISM
FINANCING RISK IN THE REPUBLIC OF ARMENIA ®**

Approved on March 26, 2010 at the meeting of the
Interagency Commission on the Fight against Counterfeiting of Money,
Fraud in Plastic Cards and Other Payment Instruments,
Money Laundering and Terrorism Financing

Restricted

ANNEX 21 - SUMMARY OF CONDUCTING A STRATEGIC ANALYSIS OF MONEY LAUNDERING AND TERRORISM FINANCING RISK IN THE REPUBLIC OF ARMENIA

1. Objectives and methodology of the strategic analysis

The main objectives of the strategic analysis of money laundering and terrorism financing (ML/FT) risk as summarized in this document are the following:

1. Clarify the possible sources, sectors, schemes and/or supporting circumstances that influence ML/TF offences and their suppression in the Republic of Armenia,
2. Enhance the direction and efficiency of AML/CFT mechanisms while readdressing them towards higher risk factors and sectors.

For these purposes, the Financial Monitoring Center of the Central Bank of the Republic of Armenia developed a methodology for conducting the strategic analysis which was approved on March 26, 2010 at the meeting of the Interagency Commission on the Fight against Counterfeiting of Money, Fraud in Plastic Cards and Other Payment Instruments, Money Laundering and Terrorism Financing. Basing on the methodology, the Interagency Commission also approved a decision to collect necessary data from authorized agencies and institutions during the following months (from 2009 statistics), analyze them and publicize the summary of results.

The analysis was conducted in seven directions as follows:

2. Predicate offences for ML/FT

In pursuance of clarifying the origins of proceeds for ML, statistics on predicate offences for ML, as specified under Article 190 of the Criminal Code of the RA, was analyzed, which provided for the evaluation of offences generating proceeds of crime in terms of their recurring involvement in possible ML schemes and the potential danger they pose. For this purpose, among all crimes recorded in 2009, the most material crimes against private property and offences generating proceeds of crime with at least 40 incidents recorded thereon were selected and taken into consideration for the conduction of the analyses.

Top 10¹ crimes that pose higher risk of ML in the Republic of Armenia are illustrated in the table presented below in the order of descending risk estimates:

¹ Data provided by the Police of the RA

Predicate offence	Number of crimes recorded with the current offence	a. Share of the current offence in the total number of crimes recorded ²	b. Share of crimes in large amounts in the total number of current offences	Risk estimate
- 1 -	- 2 -	- 3 -	- 4 -	- 5 -
Theft	3,961	0.60	0.15	0.090
Distribution of narcotics	539	0.09	0.70	0.063
Fraud	738	0.12	0.20	0.024
Tax evasion	159	0.03	0.30	0.009
Banditry	151	0.02	0.40	0.008
Illegal and false entrepreneurship	79	0.01	0.70	0.007
Squandering or embezzlement	182	0.03	0.20	0.006
Contraband	72	0.01	0.60	0.006
Robbery	265	0.04	0.12	0.005
Bribery	44	0.01	0.30	0.002

Column 2 of the table illustrates the total number of crimes recorded during 2009 with the relevant offences.

The following indicators were calculated under Columns 3 and 4 in terms of each one of the offences:

- a. the number of crimes recorded with the current offence was divided by the total number of crimes recorded with all offences in order to evaluate the share of the current offence in the total figure,
- b. the number of crimes recorded in large amounts (3,000 thousand drams and more) with the current offence was divided by the total number of crimes recorded with the same offence in order to evaluate the share of large-amount crimes in the total figure.

Column 5 of the table illustrates the numerical values for risk estimates of the offences, which have been derived as a result of multiplying indicators a. and b. as to demonstrate the periodicity of recording the current type of offence that involves significantly large proceeds of crime. The above estimates lead to a conclusion that the following predicate offences pose higher risk of money laundering in the Republic of Armenia in terms of being possible origins of proceeds of crime: those are theft, distribution of narcotics and fraud. This is also evidenced by the thematic breakdown of court verdicts issued in 2009 that include the ML/FT component.

3. Legal System

Deficiencies or inconsistencies inherent to the legal system of the RA significantly contribute to the level of ML/FT risk and act as impairment for the effective enforcement of prevention and prosecution mechanisms against such crime. The most significant deficiencies and inconsistencies that were indicated in the third round evaluation report of the AML/CFT system

² During 2009, total of 6,190 incidents were recorded with the offences presented in the table.

of the Republic of Armenia (hereinafter: Evaluation report) as approved by the Council of Europe's MONEYVAL Committee, acted as a foundation for the analysis conducted with the above purposes. The deficiencies and inconsistencies were categorized by risks inherent to legal acts of preventive and criminal-legal frameworks, as well as risks associated with existent shortcomings in legal acts and the of implementation efficiency thereof. In terms of the above, the following risks are identified:

Risks inherent to legal acts of preventive framework

- Absence of mechanisms for law enforcement authorities to obtain bank secrecy information on legal persons,
- Possibility of issuing and servicing bearer instruments without any restriction on the value,
- Absence of fit and proprietary requirements for the ownership, management and beneficial owners of casinos, organizers games of chance and lotteries,
- Time-bound mechanisms for freezing of funds or other assets related to terrorism (absence of termless freezing mechanisms).

Deficiencies in effective enforcement of legal requirements of preventive framework

- Passive reporting on suspicious transactions by non-bank financial institutions and designated non-financial businesses and professions,
- Absence of adequate supervision and sanctions imposed by supervisory authorities on designated non-financial businesses and professions in terms of AML/CFT requirements,
- Relaxed supervision of ML/FT risks and absence of sanctions imposed on non-commercial organizations.

Risks inherent to legal acts of criminal-legal framework

- Absence of legal capacity to confiscate third parties' property in the scope of criminal cases with predicate offences.

Deficiencies in effective enforcement of legal requirements of criminal-legal framework

- Absence of autonomous ML/FT cases (without combination) examined,
- Relatively low number of cases and verdicts involving offences for ML compared to the number of cases and verdicts with predicate offences of higher risk.

4. Institutional systems

The evaluation of capacities of state authorized bodies and institutions that are addressed towards ML/FT prevention and criminal prosecution is of vital importance in terms of determining the ML/FT risk in the Republic of Armenia. For this purpose, the risk has been evaluated based on both the stipulations under the Evaluation report and the data from surveys conducted at relevant bodies and institutions as well as the deficiencies in enforcing the clarified legal requirements. At that, the systemic deficiencies and shortcomings evaluated are as follows:

In courts and law enforcement authorities of the RA (Court system, Prosecution Office, National Security Service, Police, State Revenue Committee)

- Lack of practical trainings for operative investigators, inquest officers, investigators and prosecutors in the field of tactics and methodology of examining ML/FT offences, collection and verification of evidence.

- Lack of practical trainings for prosecutors in the field of defending convictions of ML/FT in courts and those for prosecutors and judges in the field of characteristics of judicial proceedings for verifying and assessing evidence for cases of ML/FT.

- Lack of technical resources (computer equipment, connections, and special devices) for operative investigators, inquest officers and investigators.

In supervisory authorities of financial institutions (Financial Supervision Department of the Central Bank of the RA)

- Lack of professional resources for scrutiny of AML/CFT related issues in the course of off-site surveillance and on site examinations at all types of financial institutions.

In supervisory authorities of designated non-financial businesses and professions (Ministry of Justice, Ministry of Finance, State Committee of Cadastre, Chamber of Advocates)

- Lack of professional resources for scrutiny of AML/CFT related issues in the course of supervision of non-financial institutions.

- Absence of supervision manuals (methodology) for each category of ML/FT risks inherent to the non-financial segments.

In the Financial Intelligence Unit (Financial Monitoring Center of the Central Bank of the RA)

- Need for upgrading the functions and processes of the Financial Monitoring Center based on the experience of other foreign financial intelligence in the field of systematizing processes.

- Presence of direct and efficient access problems to different sources of information.

5. Financial system

According to all estimates suggested by international practices, ML/FT risks of private sector are highly concentrated in the financial system considering the volume of financial assets flowing through this system, the variety of financial transactions and the ability of running transnational operations. The Republic of Armenia is not an exception from this rule where ML/FT risks and relevant schemes revealed are mainly practices in the financial sector as evidenced by the practices of the AML/CFT system in operation. The following features of different types of financial institutions were taken into consideration for the purpose of evaluating the ML/FT risk of the financial system of the Republic of Armenia: financial market share, type, quantity and average amount (in absolute value and as share in total) of transactions conducted/services provided, residency of ownership and clientele, periodicity of revealing

ML/FT schemes of suspicious transactions, etc. Summary data³ on the distribution of assets between financial system participants is presented in Annex 1 attached, while Annex 2 illustrates certain characteristics⁴ of financial system participants' businesses that provide evidence for the low level of ML/FT risk inherent to the operations thereof.

As a result of contrasting and analyzing the size of assets as a primary criterion, and other additional criteria (periodicity and volume of transactions, residency of ownership and clientele, STRs received, etc), the following volume-quantity concentration rates of assets and transactions in the financial system became apparent:

- For banks - 93-96%,
- For credit organizations, insurance companies, securities firms and money remitters - 3%-6%, and for other participants of the financial market (pawnshops, foreign exchange offices) - around 1%.

Considering the concentration rates above, as well as the fact that all participants of the financial system are supervised by a single body, that is the Central Bank, a conclusion can be drawn that the distribution of ML/FT risks and the preventive measures thereof are distributed among the segments of the financial system in the same proportion as that of the assets and additional criteria.

6. Non-financial sector

In comparison to other participants of the financial system, the risk level of designated non-financial business and professions involved in AML/CFT is significantly lower. The low level of risk is significantly evident in the Republic of Armenia due to the imperfect development of intermediated services in the non-financial sector, simple variety of services, limited turnover, foremost locally oriented nature of operations of institutions providing such services, lack of international relationships. Nevertheless, in relation to the assessment of ML/FT risk inherent to designated non-financial businesses and professions, the estimated financial turnover rates for separate segments and the possibility of involvement in suspicious ML/FT schemes were taken into consideration. At that, the following designated non-financial businesses and professions are considered of higher importance in terms of ML/FT risks:

According to 2009 statistics, total of 78⁵ *entities organizing lotteries, games of chance and casinos* were operating in Armenia, whereas the total sales revenue thereof in 2009 was 22,401,916 thousand RA drams⁶, i.e. 287,204 thousand RA drams annually in terms of each participant or in equivalence - 23,934 thousand RA drams of sales revenue per month. Considering the revenue rates above, as well as the fact that no transactions of financial nature are conducted within this segment, a conclusion can be drawn that ML/FT risks are considerably low herein.

³ "Financial system of Armenia; the development, regulation and supervision, 2009" periodic issue, Central Bank of the Republic of Armenia

⁴ Data provided by the Financial Supervision Department of the CBA

⁵ Data provided by Ministry of Finance of the RA

⁶ Net profit - 2,890,117 thousand RA drams

This conclusion can be totally applicable to *audit professionals* also. Total of 31⁷ audit professionals were operating in 2009, whereby the total sales revenue thereof in 2009 was 4,411,970 thousand RA dram⁸, i.e. 142,322 thousand RA drams annually in terms of each participant or in equivalence - 11,860 thousand RA drams of sales revenue per month.

The largest segment of the non-financial sector is the *real estate market* (total of 15,199 real estate buying and selling transactions⁹ were conducted in 2009 amounting to 196,680,213 thousand RA drams) whereas transactions therein are conducted in intermediation of notaries. On the opposite side, the following circumstances lead to a conclusion that the real estate market is posed to a moderate level of ML/FT risk:

- A unit of property with a value not exceeding 20,000 thousand RA drams was the subject of 85% of real estate buying and selling transactions conducted, whereas the underlying value of one transaction was 13,000 thousand RA dram on average,
- A significant portion of real estate buying and selling transactions is conducted in intermediation of realtors (total of 204 registered entities), whereas, total of 6 transactions amounting to 78,000 thousand RA drams are conducted by each realtor per month on average.

Statistical data on transactions conducted by *attorneys, other legal professionals, sole practitioner accountants and accounting firms, dealers in precious metals and stones* are missing; therefore risk analysis in this segment cannot be conducted.

Concurrently, the conducted analysis suggests that there is no other segment in the non-financial sector of the Republic of Armenia or any institution (entity) involved therein that would pose a significant ML/FT risk.

7. Non-commercial segment

International practices suggest that non-commercial organizations (in particular for charities) are considered to pose higher risk due to their involvement in FT schemes. This risk is considerably lower in the Republic of Armenia due to the following circumstances:

- The population of Armenia is nearly-homogenous in terms of demographics, and no preconditions exist for causing severe conflicts on inter-ethnic or other grounds. This factor does not result in a favorable environment for terrorist organizations to operate and for the involvement of non-commercial organizations in such purposes.
- Around 84% (total of 5,890 organizations) of founders and ownership of non-commercial organizations are residents of the Republic of Armenia¹⁰, whereas the total number of branches and representations of foreign organizations is 708 which round to 12% of the total number, hence a lower probability for such organizations to be involved in international FT schemes.

⁷ Data provided by the Ministry of Finance of the RA

⁸ Net profit - 499,731 thousand RA drams

⁹ Data provided by the State Committee of Real Estate Cadastre adjunct to the Government of the RA

¹⁰ Data provided by the Ministry of Justice of the RA

- The objective of majority of charities is the assistance in meeting diverse social needs of Armenian residents, citizens or organizations, and not the collection and transfer of funds to other countries, which in turn provides for the low level of FT risks in this segment.
- The volume of financial and business operations of non-commercial organizations is considerably low (average financial turnover was 7,000 thousand RA drams per organization in 2009).

8. Economic, geographic and demographic environment

The structure of economy, geographic location of the country, demographic breakdown and other aggregate factors have a significant influence on the level of ML/FT risk in the country and explain the attractiveness and involvement of the country in ML/FT schemes. Thus, the following factors among the ones mentioned above are of importance for the Republic of Armenia.

Considering the fact that one-third (1,111 thousand people)¹¹ of population (total number is 3,238 thousand people) of the Republic of Armenia resides in the capital city Yerevan, as well as the fact that 85% of trade turnover is conducted in Yerevan and the majority of financial institutions are headquartered herein, a conclusion can be drawn that, in geographic terms, ML/FT risks are concentrated in Yerevan.

Due to several estimations, the volume of shadow economy in the Republic of Armenia is around 25-30% of the GDP, which poses higher than average risk in terms of ML/FT. On the opposite side, cash in circulation is at 248,520,000 thousand RA drams on average¹², i.e. the volume of cash drams per resident of the RA is 76,000 thousand RA drams. Such volume of cash circulation (even after considering the 40% rate of dollarization) does not have a significant influence on ML/FT risk.

Non-commercial remittances received from abroad (mainly from diaspora) are of significant absolute value in the balance of payments of the Republic of Armenia, whereas the breakdown of originating countries is the following¹³: Russian Federation (80.4% of inflow), USA (5.3% of inflow), Ukraine (2.0% of inflow): Particularly, non-commercial remittances received from abroad by natural persons totalled to 1,124,119 thousand US dollars, outward remittances were 194,884 thousand US dollars, thus providing for net inflows of 929,235 thousand US dollars. Henceforth, on average, every resident of the Republic of Armenia receives 310 US dollars of remittances per year (25 US dollars per month). The findings presented lead to a conclusion that money received from abroad is used for consumer purposes mostly, thus no risk of ML/FT can present herein.

Foreign trade relations explain the presence of certain ML/FT risks inherent to import and export transactions. From this standpoint, ML/FT risks are concentrated in the following trade relations in terms of the breakdown of foreign trade turnover by countries (data on foreign trade

¹¹ Official website of the National Statistics Service (www.armstat.am)

¹² 2009 Statistics guidebook of the Central Bank of the RA

¹³ Data provided by the Statistics Department of the CBA

turnover¹⁴): EU countries - 32%, Russian Federation - 20%, China - 9.5%, USA - 4.5%, Turkey - 4%, and the remaining 30% is distributed among other countries in small proportions.

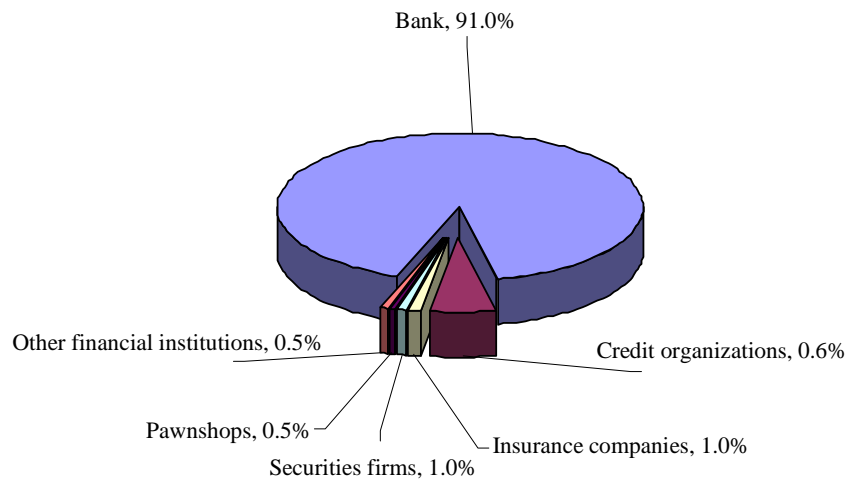
As mentioned above, the population of the Republic of Armenia is nearly-homogenous (Armenians - 97.9%, Yazidi Kurds - 1.3%, Russians - 0.5%), which does not contribute to the level of ML/FT risk in the country.

Annex 1

Data on the distribution of assets among the participants of the financial system of the RA (as of 30.06.2010)

Total assets	thousand RA drams	thousand US dollars ¹⁵	Share
Banks	1,329,239,000	3,616,977	91%
Credit organizations	86,347,000	234,958	6.0%
Insurance companies	17,239,000	46,909	1.0%
Securities firms	15,153,000	41,233	1.0%
Pawnshops	7,544,000	20,528	0.5%
Other financial institutions*	7,082,000	19,271	0.5%
Total	1,462,604,000	3,979,875	100.0%

* foreign exchange offices and money remmitters



¹⁴ Official website of the National Statistics Service (www.armstat.am)

¹⁵ The exchange rate as of 30.06.2010: USD 1 = AMD 367.5

Annex 2

Characteristics of credit organizations' operations (as of 30.06.2010)

Article	Indicator	Item
Total number of credit institutions*	29	unit
Total assets of credit organizations	86,347,000	thousand RA
Total amount of loans provided	49,831,000	thousand RA
Share of agricultural loans	24.0%	percentage
Share of business loans	21.0%	percentage
Share of mortgage loans	17.0%	percentage
Total number of loans provided	84,130	unit
Average amount of a loan provided	620	thousand RA

* Under the legislation of the RA, credit organizations are not granted a permission to collect deposits and provide payment services, and the main function thereof is the provision of loans

Characteristics of insurance companies' operations (as of 30.06.2010)

Article	Indicator	Item
Total number of insurance companies	10	unit
Total assets of insurance companies	17,239,000	thousand RA drams
Total number of insurance payouts in the first half of 2010	14,990	unit
Total amount of insurance payouts in the first half of 2010	783,647	thousand RA drams
Average amount of an insurance payout	52	thousand RA drams

* All insurance companies are exceptionally out of life insurance business

Characteristics of securities firms' operations (as of 30.06.2010)

Article	Indicator	Item
Total number of securities firms*	8	unit
Total assets of securities firms	15,153,000	thousand RA drams
Share of government bonds in the securities market	88.0%	percentage

* Securities firms other than banks

Characteristics of pawnshops' operations (as of 30.06.2010)

Article	Indicator	Item
Total number of pawnshops	117	unit
Total assets of pawnshops	7,554,000	thousand RA drams
Total amount of loans provided	7,374,000	thousand RA drams
Share of loans against gold	89.0%	percentage
Average number of loans provided a day	26	unit
Average amount of a loan provided	81	thousand RA drams

Characteristics of foreign exchange offices' operations (as of 30.06.2010)

Article	Indicator	Item
Total number of foreign exchange offices	302	unit
Total assets of foreign exchange offices	5,144,000	thousand RA drams
Average amount of a transaction	120	thousand RA drams

Characteristics of money remitters' operations (as of 30.06.2010)

Article	Indicator	Item
Total number of money remitters	10	unit
Total assets of money remitters	1,938,000	thousand RA drams
Average amount of a transaction	170	thousand RA drams

**ANNEX 22 – EXTRACT FROM PROTOCOL N 6 OF OCTOBER 21,
2009 ON ENSURING THE IMPLEMENTATION OF DECISIONS
APPROVED ON OCTOBER 21, 2009 AT THE MEETING OF THE
BOARD OF THE PROSECUTION OFFICE OF THE REPUBLIC OF
ARMENIA®**

Restricted

ANNEX 23 - GUIDANCE FOR SOLE PRACTITIONER ACCOUNTANTS, ACCOUNTING FIRMS AND SOLE PRACTITIONER AUDITORS, AUDITING FIRMS ON MINIMAL REQUIREMENTS FOR ASSESSING AND PREVENTING MONEY LAUNDERING AND TERRORISM FINANCING RISKS

**Approved by the Decision of the
Chairman of the Central Bank of the
Republic of Armenia, No 1/875 - A of August 6, 2010**

Introduction

1. This Guidance is presented based on Part 2, Article 11 of the Republic of Armenia Law on Combating Money Laundering and Terrorism Financing (hereinafter referred to as the Law) and is applicable to reporting entities such as sole practitioner accountants, accounting firms and sole practitioner auditors, auditing firms (hereinafter referred to as reporting entities) as defined by Article 3 of the Law. The Guidance presents specific criteria of money laundering and terrorism financing (hereinafter also referred to as ML/TF) risks inherent to reporting entities, and the prevention mechanisms thereof.

2. The purposes of identifying and assessing ML/TF inherent risks and taking commensurate preventive measures by reporting entities are the following:

- 1) Reporting entities would safeguard their high rating and reputation in the view of the clients and the public, with the reasoning that in practice they are engaged exceptionally in legitimate activities.
- 2) The mechanisms prescribed by the Guidance would enable reporting entities to discern their higher risk clients and to take actions which would not impede their own activities aimed at making profit on one hand and would prevent possible risks arising from such clients on the other hand.
- 3) Reporting entities would be safeguarded from possible future allegations of being involved in or facilitating different money laundering schemes, with the reasoning that they have effective systems in place for assessing and preventing ML/TF risks.

3. The Guidance also defines a comprehensive set of measures for reporting entities, which, when realized, would ensure compliance of their practices with requirements of the Law. At that, as prescribed by the Law, provisions set forth under the Guidance are applicable to reporting entities only in terms of services involving the following transactions prepared or carried out for the client:

- 1) Buying and selling of real estate,

- 2) Managing of client money, securities or other assets,
 - 3) Managing of bank and securities accounts,
 - 4) Provision of funds or other assets for the establishment, operation, or management of legal persons,
 - 5) Provision of services for the establishment, operation, or management of legal persons, as well as for the alienation (acquisition) of stocks (equities, shares and the like) in the statutory (equity and the like) capital of legal persons, or for the alienation (acquisition) of stock issues (stocks, shares and the like) of legal persons at a nominal or market value;
4. Concepts referred to in the Guidance are used in accordance with the concepts and formulations defined by the Law.

Section 1: Risks

Chapter 1: Importance of Categorizing and Managing Risks

5. ML/TF risks faced by reporting entities vary depending on many factors including the professional activity of reporting entities, the type and identity of clients, the nature of relationships with clients, and the methods for providing services (for the purposes of this Guidance, the concept of service corresponds to that of business relationship as defined by the Law). The minimal comprehensive set of risks and their prevention mechanisms are defined by the Law.
6. Reporting entities should precisely identify the ML/TF risks and their prevention measures, which may be relevant in the course of their activities. Concurrently, every practical case or situation may give rise to new risks; therefore, the prevention measures must be dynamically developing ones.
7. Reporting entities may face higher or lower risk criteria.
8. Higher risk criteria, in turn, are classified into country or geographic, client, and transaction risk categories. These risk categories should not be considered separately, in isolation from one another, as for the presence of a higher risk criterion in one of the categories can lead to the presence of a higher risk criterion in another risk category or affect the possibility of the emergence of such. Besides, the same service provided by a reporting entity is possibly to simultaneously comprise more than one risk criterion pertaining to one or several risk categories.
9. Based on own knowledge and experience, reporting entities should be able to identify existent ML/TF risks, assess each one of them and aggregate a comprehensive risk assessment for the services offered or provided.
10. Different categories of risks are presented under this Guidance with the following purposes:
- 1) To illustrate a minimal set of risks and, based on that, propose a model package of risk prevention measures;
 - 2) To precisely identify ML/TF risks inherent to reporting entities by means of evaluating risks specified under the Guidance from the standpoint of their own practices.

Chapter 2: Country or Geographic Risk

11. There is no research conducted by any international organization that would designate a particular country or geographic area as undoubtedly and unconditionally presenting higher ML/TF risk for reporting entities. Nevertheless, the following countries and territories are considered to pose higher risk in terms of ML/TF:

- 1) Countries and territories subject to sanctions, embargoes, or similar restrictive measures issued by the UN¹⁶;
- 2) Countries and territories publicized by the FATF and FATF-style regional bodies as lacking or having inefficient AML/CFT systems¹⁷.
- 3) Countries and territories publicized by international structures as having significant levels of corruption¹⁸.
- 4) Countries and territories included in the list of off-shore jurisdictions as approved by the Central Bank of the Republic of Armenia¹⁹.

12. Reporting entities should consider the above-listed countries and territories as posing higher risk if:

- 1) Clients, authorized persons, beneficial owners are residing or located in these countries and territories, or clients that have business relationships with them,
- 2) The source of income and (or) wealth of clients is in these countries or territories,
- 3) These countries and territories are the place for the conduction of the business relationship and (or) transaction.

13. Besides the above, reporting entities may, based on own experience and practices, classify/consider any country or geographic area as posing higher risk, even if it is not listed under the above-specified criteria.

Chapter 3: Client Risk

14. Every reporting entity should have a clear understanding of which category of clients or which particular client poses higher ML/TF risk. In this sense, clients posing higher risk include:

- 1) Politically exposed persons²⁰;

¹⁶ The FMC official web-site contains links to documents issued by the UN Security Council Sanctions Committee (www.cba.am/Financial_Monitoring_Center). Documents are available at www.un.org/sc/committees.

¹⁷ The FMC official web-site contains links to FATF and MONEYVAL publications (www.cba.am/Financial_Monitoring_Center). The publications are available at www.fatf-gafi.org, www.coe.int/moneyval.

¹⁸ See, for example, at www.transparency.org. The FMC official web-site contains links to data issued by Transparency International (www.cba.am/Financial_Monitoring_Center).

¹⁹ See Republic of Armenia Central Bank Board Decision No 28, of July 28, 2009.

- 2) Corporate clients with unnecessarily complex control structure of management bodies or beneficial owners that are impossible to identify;
- 3) Corporate clients with inexplicably frequent changes in members of management or ownership or clients with owners that are residents of countries or territories posing higher risk;
- 4) Clients that are cash intensive businesses (e.g. casinos, gas stations, hotels, etc.);
- 5) Resident or non-resident non-profit organizations (including charities), where there is:
 - a. No apparent corporate structure resulting in considerable divergence from the requirements specified under the applicable legislation; and (or)
 - b. No authorized supervisory body entitled to examine financial and business operations of these organizations and impose responsibility measures for the violations disclosed;
- 6) Clients with members of management that have been convicted for willfully committed crimes, if this circumstance becomes known to the reporting entity in the course of conducting professional activities;
- 7) Clients having numerously changed the address of their permanent living (registration), location, or business;
- 8) Legal persons having factually conducted no activity during a considerable period of time;
- 9) Shell companies having state registration but no factual address of location or any activity conducted;
- 10) Clients with multijurisdictional operations that do not have adequate centralized corporate oversight or control.

Chapter 4: Transaction Risk

15. Certain transactions conducted by clients may pose higher ML/TF risks for reporting entities. These include cases when:

- 1) Transactions are conducted by the client, where the price is apparently lower or higher than the real/market price of the subject of transaction (e.g. a real estate buying or selling contract is signed at an apparently low price);
- 2) Payment against a transaction is unreasonably made to the client by an un-associated party or funds are transferred (provided) to the client with no business rationale;

²⁰ The definition of politically exposed persons is stipulated by the Law, while relevant information can be found from various public sources, such as the search engine of www.google.am, the official web-site of the US Central Intelligence Agency (www.cia.gov/library/publications/the-world-factbook), web-sites of relevant governmental bodies of different countries, etc. Besides these, there are also different paid information databases (e.g. World-Check, Factiva, Accuity), which provide most comprehensive information on politically exposed persons. The FMC official web-site contains links to the stated information resources (www.cba.am/Financial Monitoring Center).

- 3) Payments against transactions are often made in cash (using cash method) by corporate clients, whereas in such conditions transactions are usually carried out by means of non-cash payments (e.g. large-scale purchases of consumer electronics for office use);
- 4) Clients provide apparently fake or incomplete information about the real objectives, nature, and subject of the transactions carried out;
- 5) Clients carry out transactions that are apparently not commensurate to their business profile (e.g. a company providing tourism services signs contracts for importing manufacturing equipment);
- 6) Transactions are carried out where parties (to be) involved (would) maintain their anonymity (e.g. contracts are signed with companies incorporated in off-shore jurisdictions that have nominal founders and directors);
- 7) Transactions are carried out assuming complicated or unreasonably mediated flow of funds (e.g. payments against importing equipments are made to foreign intermediary vehicles in several tranches, which in their turn, are obliged to pay the amount to the exporting company);
- 8) Clients possess insufficient technical and human resources compared to the nature or volumes of their activities (e.g. a company conducts wholesale business of processing and exporting jewelry, but has only three employees);
- 9) Business activities and financial turnover of clients take place in unreasonable seasonality;
- 10) Clients running business with unprecedented and unreasonable profits or losses;
- 11) Financial transactions of clients are unreasonably structured (e.g. payments arising from the same contract are unreasonably received in two simultaneous transfers);
- 12) Apparent discrepancies exist in invoices of clients (in product descriptions or payable amounts);
- 13) Accounting or auditing services are offered to be provided with unreasonable urgency.

Chapter 5: Lower Risk Criteria

16. Reporting entities can consider only the following clients as characterized by lower risk criteria (except for the clients residing or located in countries and territories lacking or having inefficient AML/CFT systems):

- 1) Financial institutions effectively supervised in terms of combating money laundering and terrorism financing,
- 2) Governmental bodies,
- 3) Local self-government bodies,
- 4) State-owned non commercial organizations,
- 5) Public administration institutions.

Chapter 6: Variables That May Impact Risk Criteria

17. ML/TF risks inherent to practices of reporting entities and resources in place for their mitigation are all dependant on the size, sphere, expertise and other conditions of their activities. For example, ML/TF risks and mitigation resources for a sole practitioner accountant or auditor will be different from that of a large accounting or auditing firm. Therefore, every reporting entity should precisely identify the circumstances having impact on the formation of ML/TF risk criteria in the course of his practices. Typical examples of such circumstances are:

- 1) Nature (one-time or recurrent), duration, regularity, and periodicity of services offered or provided;
- 2) Robustness of the legal regime (e.g. licensing, registration rules) applicable to the clients,
- 3) Rating and business reputation of the client;
- 4) Nature of the accounting or auditing services offered (services provided on-site or by distant communication);
- 5) Client residency and, in case of foreign clients, the nature of their relation with the Republic of Armenia;
- 6) Circumstances related to introducing the client (whether the client has been recommended to the reporting entity by another reputable or familiar party, or has applied without prior appointment);
- 7) Presence of more than one higher or lower risk criterion within the service provided to the client.

Section 2: Risk Prevention Measures

Chapter 7: Internal Monitoring Function for Prevention of Risk

18. For the purpose of effective prevention of ML/TF risks specified under Section 1 of this Guidance, reporting entities should introduce an internal monitoring function. At that, in order to appropriately realize this function, in accordance with Article 22 of the Law, reporting entities shall be obligated to have an internal monitoring unit or an employee responsible for dealing with the prevention of ML/TF, or otherwise outsource this function to relevant specialized entities (hereinafter referred to as internal monitoring unit).

19. Article 22 of the Law shall be applicable to reporting entities with the following differences:

- 1) In case of sole practitioner accountants and auditors, the internal monitoring function of ML/TF prevention should be performed by the sole practitioner accountants and auditors themselves;
- 2) In case there is specialized staff available, the function may be assigned to an individual employee or a structural unit. In this case, the autonomy and direct accountability of the internal monitoring unit to the senior management of the reporting entities should be ensured.

20. The unit performing internal monitoring functions of a reporting entity should at least undertake the following measures:

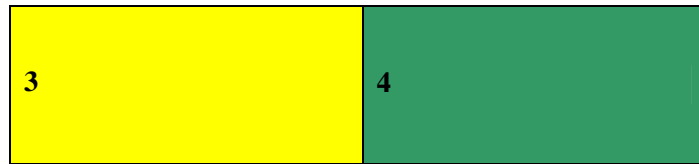
- 1) Develop AML/CFT internal legal acts (in case of having more than 10 employees); present proposals on enhancing effectiveness of such acts;
 - 2) Categorize clients and services provided to them in terms of ML/TF risk exposure in accordance with the Law, this Guidance, and internal legal acts of the reporting entity; build up awareness among employees of the reporting entity about specific categories of risks, and higher risk clients and services;
 - 3) Provide for regulation and effectiveness of client due diligence processes, including enhanced and simplified due diligence, as well as for the ongoing monitoring of clients and of the business profile thereof, information recording, maintenance, and updating processes;
 - 4) Conduct analysis in relation to recognizing a transaction or business relationship as suspicious;
 - 5) Make the final decision with regard to recognizing a transaction or business relationship as suspicious, to rejecting or suspending them, as well as to freezing of funds or other assets associated to terrorism;
 - 6) Ensure the filing of suspicious transaction or business relationship reports with the Financial Monitoring Center of the Central Bank of the Republic of Armenia (hereinafter referred to as the Financial Monitoring Center);
 - 7) Undertake other measures of risk prevention as prescribed under this Section.
21. The structural unit of reporting entities performing the functions of internal monitoring should have direct and timely access to any document or information in relation to services provided by reporting entities.

Chapter 8: Risk Assessment Methods

22. Before providing services to clients and during the entire duration of in-progress contractual services, reporting entities should assess the aggregate ML/TF risk exposure in relation to them. In the course of assessing client and transaction risk, the following matrix is recommended as a guide in order to consider risk criteria and circumstances having impact on them, as specified under Section 1 of this Guidance.

	<i>Negative Set of Circumstances Having Impact on Risk</i>	<i>Positive Set of Circumstances Having Impact on Risk</i>
<i>Higher Risk Criteria Stance</i>	1	2

Lower Risk Criteria Stance



- 1) Situation 1 suggests that the service offered or provided poses higher risk. For the purpose of determining risk exposure, it is also important to consider what the higher risk criteria are and how many of such criteria are present. In this case, the question of filing a suspicious transaction or business relationship report with the Financial Monitoring Center should also be considered and, regardless of the decision made, the outcomes of such consideration should be documented and maintained.
 - 2) Situation 2 suggests that the service offered or provided may pose a higher risk, although circumstances having impact on it are of positive nature within the given set of risks. In this case, again, for the purpose of determining risk exposure both the number and nature of higher risk criteria and the impact of the positive set of circumstances should be considered.
 - 3) Situation 3 suggests that the service offered or provided poses medium risk, although certain circumstances are present, which may in future transform it into higher risk. In this case, it is important to establish enhanced ongoing monitoring over the service, as well as to conduct enhanced due diligence with the purpose of effectively controlling possible fluctuations in risk exposure.
 - 4) Situation 4 suggests that the service offered or provided poses lower risk, and there is no material circumstance implying the possible presence of high risk criteria.
23. At that, if the service offered or provided comprises both higher and lower risk criteria, the aggregate risk exposure should be determined through assessing the nature and materiality of each risk criterion involved, as well as of the set of circumstances having impact on risk.

Chapter 9: General Rules for Client Due Diligence

24. Client due diligence or the principle “Know Your Client” is intended to ensure that reporting entities have adequate and comprehensive awareness of the real identity of their clients. This applies to identifying not only the clients, but also the authorized persons acting on behalf of them and the beneficial owners (if any).
25. Client due diligence should be conducted in each and every case of offering or providing a service, whether such service involves higher, medium, or lower risk. Client due diligence shall be required for both new and existing clients within the scope of services provided to them.
26. Article 15 of the Law defines the cases, the procedures, and the required minimum documentation for conducting client due diligence by reporting entities. Client due diligence shall comprise the following measures (Articles 15, 16 and 20 specify the requirements within the scope of each measure):

- 1) In accordance with Article 15 of the Law, obtain information on the identity (identification) of clients (including the authorized person acting on behalf of the client and the beneficial owner) and verifying the accuracy of the information obtained;
- 2) In accordance with Article 16 of the Law and Chapter 10 of this Guidance, perform ongoing monitoring of the business relationship (service);
- 3) In accordance with Article 15 of the Law and Chapters 11 and 12 of this Guidance, undertake measures based on risk-based approach for client due diligence.

27. At that, measures specified by Sub-Clause 1, Clause 26 of this Guidance shall be undertaken by reporting entities before providing services to clients. In exceptional circumstances, when the ML/TF risk is effectively prevented, and where it is essential not to impair the normal course of services provided to clients, measures towards obtaining information on the identity of the client and verification of such information may be undertaken after the service is actually provided, within a reasonable timeframe of not more than seven days.

Chapter 10: Ongoing Monitoring of Business Relationship (Service)

28. An essential constituent of client due diligence is the ongoing monitoring of clients and their business profile in the whole course of business relationships (services) provided by reporting entities, so as to form a complete and clear understanding of the purpose and the expected nature of the services provided. For this purpose, depending on the ML/TF risk exposure of the service provided by reporting entities, the following measures shall be undertaken by them during the whole course of providing the service:

- 1) Verify the interconnection between transactions carried out within the scope of the service provided, detect possible schemes for these connections, as well as determine the objective of the transactions;
- 2) Verify whether the nature of the transactions is commensurate to the type of business activities of the client;
- 3) Check the categories, periodicity, and chronology of transactions carried out in a standard unit of time;
- 4) Verify possible interrelations between the parties of transactions, the authorized persons, as well as the beneficial owners;
- 5) Verify the existence of transactions by means of which clients pursue to avoid being reported to the Financial Monitoring Center by reporting entities;
- 6) Obtain possibly complete information, as necessary, on the sources of income and (or) wealth of clients, and on the changes thereof;
- 7) Compare the sources, turnover, and amounts of funds of the client subject to different transactions;
- 8) Assess possible ML/TF risks in services offered or provided, by means of comparison with the criteria and typologies of suspicious transactions and business relationships.

29. Information obtained within the scope of conducted client due diligence (including enhanced and simplified due diligence) should be updated by reporting entities at a periodicity set by them, but not less than once a year, to ensure that it is up-to-date and relevant.

Chapter 11: Enhanced Client Due Diligence

30. In case the service offered or provided poses higher risk, reporting entities should, in addition to client due diligence measures prescribed under Chapter 9 of this Guidance, conduct enhanced client due diligence.

- 1) Enhanced client due diligence should include the following measures:
 - a. Obtain senior management approval before establishing and for continuing business relationships with such clients, as well as in cases when later on it is found out that clients and (or) the beneficial owners pose higher risk, or that the transactions or business relationships comprise such criteria;
 - b. Undertake necessary actions for verifying the source of income and (or) wealth of clients;
 - c. Scrutinize, record in writing, and maintain the grounds and conditions for the following transactions, so as to permit reconstruction of transaction details in future and, of necessary, dissemination of those to authorized bodies. Such transactions include:
 - All complex and unusually large transactions, as well as unusual patterns of transactions with no business rationale or legitimate purpose;
 - Transactions involving persons residing (located) in foreign countries or territories, where international requirements for combating money laundering and terrorism financing are absent or ineffectively implemented;
 - d. Conduct enhanced ongoing monitoring of business relationships.
- 2) Enhanced client due diligence may include the following measures:
 - a. Scrutinize the required documents (information), stipulated in case of offering and providing services, in a more comprehensive and thorough manner;
 - b. Make requests to authorized government bodies with the purpose of verifying the accuracy of information on clients, transactions with and services provided to them.

31. By means of enhanced client due diligence, reporting entities should obtain reasonable clarifications and explanations, so as to form a complete and clear understanding of the clients and the services offered or provided in relation to them.

Chapter 12: Simplified Client Due Diligence

32. In case of lower risk criteria, reporting entities may perform simplified client due diligence.

33. Simplified client due diligence shall be the limited implementation of client due diligence measures performed by reporting entities, whereby the following information shall be obtained as part of the identification and verification of identity:

- 1) For natural persons - forename, surname and identification document information;
- 2) For legal persons – company name and state registration certificate number;
- 3) For government bodies and local self-government bodies - name.

Chapter 13: Minimal Requirements for Recording and Maintaining Information

34. Reporting entities should record and maintain the information specified under Chapters 9-12 of this Guidance in a manner sufficient to permit reconstruction of individual transactions so as to provide, if necessary, procedural evidence.

35. Information may be maintained in documentary form, on computers, or other electronic means.

36. Reporting entities should ensure the security and secrecy of the information recorded and maintained, and should prevent it from unauthorized use or control.

37. Reporting entities should maintain the information specified under Article 20 of the Law, including the process of review (conducted analysis) for recognizing a transaction or business relationship as suspicious as specified under Clause 42 of this Guidance.

Chapter 14: Obligation in Relation to Suspicious Transaction or Business Relationship

38. From the moment of recognizing a transaction or business relationship as suspicious, reporting entities shall be obligated to file a suspicious transaction or business relationship report with the Financial Monitoring Center.

39. To recognize a transaction or a business relationship as suspicious, reporting entities should consider the criteria and (or) typologies of suspicious transactions or business relationships.

40. Legislative requirements in relation to suspicious transaction or business relationship reports are specified:

- 1) Under Articles 4-7 of the Law establishing that reporting entities shall be obligated to file a report with the Financial Monitoring Center in case of a suspicious transaction or business relationship;
- 2) Under Decision No17-N, of January 27, 2009 of the Board of the Central Bank of the Republic of Armenia establishing the Form No 025 for reporting suspicious transaction

- or business relationship by reporting entities, the rules and deadlines for its submission, as well as the rules for the registration of reporting entities,
- 3) Under Decision No1/886A, of September 3, 2008 of the Chairman of the Central Bank of the Republic of Armenia defining suspicious transaction criteria for all reporting entities, including reporting entities for the purpose of the Guidance.
41. Reporting entities may also recognize a transaction or business relationship as suspicious, when such suspicion does not arise from any specific criteria and (or) typology of a suspicious transaction or business relationship, but its logic or pattern (dynamics) of implementation give the grounds to suspect that it is being carried out or established for the purpose of money laundering or terrorism financing.
42. In the presence of a criteria or typology of suspicious transaction or business relationship, as well as in the cases specified under Clause 41 of this Guidance, reporting entities should consider recognizing the transaction or business relationship as suspicious. If, due to such consideration, the transaction or business relationship is not recognized as suspicious, the process of review (conducted analysis) and the findings shall be documented and maintained in the manner and timeframe established by the Law and this Guidance.

ANNEX 24 - GUIDANCE for ENTITIES ENGAGED IN REALTOR ACTIVITIES ON MINIMAL REQUIREMENTS FOR ASSESSING AND PREVENTING MONEY LAUNDERING AND TERRORISM FINANCING RISKS

**Approved by the Decision of the
Chairman of the Central Bank of the
Republic of Armenia, No 1/876 - A of August 6, 2010**

Introduction

1. This Guidance is presented based on Part 2, Article 11 of the Republic of Armenia Law on Combating Money Laundering and Terrorism Financing (hereinafter referred to as the Law) and is applicable to reporting entities such as entities engaged in realtor activities (hereinafter referred to as realtors) as defined by Article 3 of the Law. The Guidance presents specific criteria of money laundering and terrorism financing (hereinafter also referred to as ML/TF) risks inherent to realtors, and the prevention mechanisms thereof.
2. The purposes of identifying and assessing ML/TF inherent risks and taking commensurate preventive measures by realtors are the following:
 - 1) Realtors would safeguard their high rating and reputation in the view of the clients and the public, with the reasoning that in practice they are engaged exceptionally in legitimate activities.
 - 2) The mechanisms prescribed by the Guidance would enable realtors to discern their higher risk clients and to take actions which would not impede their own activities aimed at making profit on one hand and would prevent possible risks arising from such clients on the other hand.
 - 3) Realtors would be safeguarded from possible future allegations of being involved in or facilitating different money laundering schemes, with the reasoning that they have effective systems in place for assessing and preventing ML/TF risks.
3. The Guidance also defines a comprehensive set of measures for realtors, which, when realized, would ensure compliance of their practices with requirements of the Law. At that, as prescribed by the Law, provisions set forth under the Guidance are applicable to realtors only in terms of transactions related to buying and selling of real estate.
4. Concepts referred to in the Guidance are used in accordance with the concepts and formulations defined by the Law.

Section 1: Risks

Chapter 1: Importance of Categorizing and Managing Risks

5. ML/TF risks faced by realtors vary depending on many factors including the professional activity of realtors, the type and identity of clients, the nature of relationships with clients, and the methods for providing services (for the purposes of this Guidance, the concept of service corresponds to that of business relationship as defined by the Law). The minimal comprehensive set of risks and their prevention mechanisms are defined by the Law.

6. Realtors should precisely identify the ML/TF risks and their prevention measures, which may be relevant in the course of their activities. Concurrently, every practical case or situation may give rise to new risks; therefore, the prevention measures must be dynamically developing ones.

7. Realtors may face higher or lower risk criteria.

8. Higher risk criteria, in turn, are classified into country or geographic, client, and transaction risk categories. These risk categories should not be considered separately, in isolation from one another, as for the presence of a higher risk criterion in one of the categories can lead to the presence of a higher risk criterion in another risk category or affect the possibility of the emergence of such. Besides, the same service provided by a realtor is possibly to simultaneously comprise more than one risk criterion pertaining to one or several risk categories.

9. Based on own knowledge and experience, realtors should be able to identify existent ML/TF risks, assess each one of them and aggregate a comprehensive risk assessment for the services offered or provided.

10. Different categories of risks are presented under this Guidance with the following purposes:

- 1) To illustrate a minimal set of risks and, based on that, propose a model package of risk prevention measures;
- 2) To precisely identify ML/TF risks inherent to realtors by means of evaluating risks specified under the Guidance from the standpoint of their own practices.

Chapter 2: Country or Geographic Risk

11. There is no research conducted by any international organization that would designate a particular country or geographic area as undoubtedly and unconditionally presenting higher ML/TF risk for realtors. Nevertheless, the following countries and territories are considered to pose higher risk in terms of ML/TF:

- 1) Countries and territories subject to sanctions, embargoes, or similar restrictive measures issued by the UN²¹;

²¹ The FMC official web-site contains links to documents issued by the UN Security Council Sanctions Committee (www.cba.am/Financial_Monitoring_Center). Documents are available at www.un.org/sc/committees.

- 2) Countries and territories publicized by the FATF and FATF-style regional bodies as lacking or having inefficient AML/CFT systems²²;
 - 3) Countries and territories publicized by international structures as having significant levels of corruption²³;
 - 4) Countries and territories included in the list of off-shore jurisdictions as approved by the Central Bank of the Republic of Armenia²⁴.
12. Realtors should consider the above-listed countries and territories as posing higher risk if:
- 1) Clients, authorized persons, beneficial owners are residing or located in these countries and territories;
 - 2) Real estate under transactions are located in these countries or territories;
 - 3) Source of income and (or) wealth of clients is in these countries or territories,
 - 4) These countries and territories are the places for conduction of transactions.
13. Besides the above, realtors may, based on own experience and practices, classify/consider any country or geographic area as posing higher risk, even if it is not listed under the above-specified criteria.

Chapter 3: Client Risk

14. Every realtor should have a clear understanding of which category of clients or which particular client poses higher ML/TF risk. Screening of the other party of transactions carried out with clients should also be of importance for realtors, as the higher risk of the other party can affect the level of risk of clients. In this sense, clients posing higher risk include:
- 1) Politically exposed persons²⁵;
 - 2) Corporate clients with unnecessarily complex control structure of management bodies or beneficial owners that are impossible to identify;
 - 3) Clients that are cash intensive businesses (e.g. casinos, gas stations, hotels, etc.);
 - 4) Resident or non-resident non-profit organizations (including charities), where there is:
 - a. No apparent corporate structure resulting in considerable divergence from the requirements specified under the applicable legislation; and (or)

²² The FMC official web-site contains links to FATF and MONEYVAL publications ([www.cba.am/Financial Monitoring Center](http://www.cba.am/Financial_Monitoring_Center)). The publications are available at www.fatf-gafi.org, www.coe.int/moneyval.

²³ See, for example, at www.transparency.org. The FMC official web-site contains links to data issued by Transparency International ([www.cba.am/Financial Monitoring Center](http://www.cba.am/Financial_Monitoring_Center)).

²⁴ See Republic of Armenia Central Bank Board Decision No 28, of July 28, 2009.

²⁵ The definition of politically exposed persons is stipulated by the Law, while relevant information can be found from various public sources, such as the search engine of www.google.am, the official web-site of the US Central Intelligence Agency (www.cia.gov/library/publications/the-world-factbook), web-sites of relevant governmental bodies of different countries, etc. Besides these, there are also different paid information databases (e.g. World-Check, Factiva, Accuity), which provide most comprehensive information on politically exposed persons. The FMC official web-site contains links to the stated information resources ([www.cba.am/Financial Monitoring Center](http://www.cba.am/Financial_Monitoring_Center)).

- b. No authorized supervisory body entitled to examine financial and business operations of these organizations and impose responsibility measures for the violations disclosed;
- 5) Clients convicted for willfully committed crimes, if this circumstance becomes known to the realtor in the course of conducting professional activities;
- 6) Clients having numerously changed the address of their permanent living (registration), location, or business;
- 7) Legal persons having factually conducted no activity during a considerable period of time;
- 8) Shell companies having state registration but no factual address of location or any activity conducted.

Chapter 4: Transaction Risk

15. Certain transactions conducted by realtors for their clients may pose higher ML/TF risks. These include cases when:

- 1) Transaction is offered, where the price is apparently lower or higher than the real/market price of the subject of transaction (e.g. arranging a real estate selling contract of a 100 square meter apartment in Yerevan at a price of 5 million drams);
- 2) There are relatively short intervals between the buying and selling of real estate or other subsequent transactions (e.g. one or several weeks/months);
- 3) Final or intermediary sources of payments against transactions are unclear or suspicious,
- 4) Payment to realtors for completing a transaction, or payment to clients against a transaction, is unreasonably made by a party un-associated with the client;
- 5) Corporate clients provide for making cash payments to realtors or to other parties to transactions;
- 6) Clients provide apparently fake or incomplete information about the real objectives, nature, and subject of the transactions carried out;
- 7) Clients promise to pay unreasonably high fees for transactions carried out, except for the cases of wealthy clients promising bonuses for successful completion of transactions;
- 8) Transactions are carried out that are apparently not commensurate to the business profile of the client (e.g. a client engaged in agricultural production processing requests to buy a hotel);
- 9) Structured payments (with several installments) against transactions are made or offered with no business rationale or legitimate purpose.
- 10) Apparently fraudulent or fake transaction is offered or conducted (e.g. a gratuitous contract is signed for an operating factory or office).

Chapter 5: Lower Risk Criteria

16. Realtors can consider only the following clients as characterized by lower risk criteria (except for the clients residing or located in countries and territories lacking or having inefficient AML/CFT systems):

- 1) Financial institutions effectively supervised in terms of combating money laundering and terrorism financing,
- 2) Governmental bodies,
- 3) Local self-government bodies,
- 4) State-owned non commercial organizations,
- 5) Public administration institutions.

Chapter 6: Variables That May Impact Risk Criteria

17. ML/TF risks inherent to practices of realtors and resources in place for their mitigation are all dependant on the size, sphere, expertise and other conditions of their activities. For example, ML/TF risks and mitigation resources for a sole practitioner realtor will be different from that of a large firm providing realtor services. Therefore, every realtor should precisely identify the circumstances having impact on the formation of ML/TF risk criteria in the course of his practices. Typical examples of such circumstances are:

- 1) Purpose (e.g. whether it is a residential property or a large factory) and location (whether it is in Yerevan or in border-line regions) of the real estate under the transaction;
- 2) Nature (one-time or recurrent), duration, regularity, and periodicity of services offered or provided;
- 3) Robustness of the legal regime (e.g. licensing, registration rules) applicable to the clients,
- 4) Rating and business reputation of the client;
- 5) Nature of communication with clients while providing realtor services (non- or face to face communication);
- 6) Client residency and, in case of foreign clients, the nature of their relation with the Republic of Armenia;
- 7) Circumstances related to introducing the client (whether the client has been recommended to the realtor by another reputable or familiar party, or has applied without prior appointment);
- 8) Presence of more than one higher or lower risk criterion within the service provided to the client.

Section 2: Risk Prevention Measures

Chapter 7: Internal Monitoring Function for Prevention of Risk

18. For the purpose of effective prevention of ML/TF risks specified under Section 1 of this Guidance, realtors should introduce an internal monitoring function. At that, in order to appropriately realize this function, in accordance with Article 22 of the Law, realtors shall be obligated to have an internal monitoring unit or an employee responsible for dealing with the prevention of ML/TF, or otherwise outsource this function to relevant specialized entities (hereinafter referred to as internal monitoring unit).

19. Taking into consideration that the size of activities and human resources of realtors are significantly inferior to the relevant characteristics of financial institutions and that, in addition, there are profound differences in terms of activities and human resources amongst realtors (from a sole practitioner realtor to a large firm providing realtor services), Article 22 of the Law shall be applicable to realtors with the following differences:

1) In case of sole practitioner realtors, the internal monitoring function of ML/TF prevention should be performed by the sole practitioner realtors themselves;

2) In case there is specialized staff available, the function may be assigned to an individual employee or a structural unit. In this case, the autonomy and direct accountability of the internal monitoring unit to the senior management of the realtor should be ensured.

20. The unit performing internal monitoring functions of a realtor should at least undertake the following measures:

- 1) Develop AML/CFT internal legal acts (in case of having more than 10 employees); present proposals on enhancing effectiveness of such acts;
- 2) Categorize clients and services provided to them in terms of ML/TF risk exposure in accordance with the Law, this Guidance, and internal legal acts of the realtor; build up awareness among employees of the realtor about specific categories of risks, and higher risk clients and services;
- 3) Provide for regulation and effectiveness of client due diligence processes, including enhanced and simplified due diligence, as well as for the ongoing monitoring of clients and of the business profile thereof, information recording, maintenance, and updating processes;
- 4) Conduct analysis in relation to recognizing a transaction or business relationship as suspicious;
- 5) Make the final decision with regard to recognizing a transaction or business relationship as suspicious, to rejecting or suspending them, as well as to freezing of funds or other assets associated to terrorism;
- 6) Ensure the filing of suspicious transaction or business relationship reports with the Financial Monitoring Center of the Central Bank of the Republic of Armenia (hereinafter referred to as the Financial Monitoring Center);
- 7) Undertake other measures of risk prevention as prescribed under this Section.

21. The structural unit of realtors performing the functions of internal monitoring should have direct and timely access to any document or information in relation to services provided by realtors.

Chapter 8: Risk Assessment Methods

22. Before providing services to clients and during the entire duration of in-progress contractual services, realtors should assess the aggregate ML/TF risk exposure in relation to them. In the course of assessing client and transaction risk, the following matrix is recommended as a guide in order to consider risk criteria and circumstances having impact on them, as specified under Section 1 of this Guidance.

	<i>Negative Set of Circumstances Having Impact on Risk</i>	<i>Positive Set of Circumstances Having Impact on Risk</i>
<i>Higher Risk Criteria Stance</i>	1	2
<i>Lower Risk Criteria Stance</i>	3	4

- 1) Situation 1 suggests that the service offered or provided poses higher risk. For the purpose of determining risk exposure, it is also important to consider what the higher risk criteria are and how many of such criteria are present. In this case, the question of filing a suspicious transaction or business relationship report with the Financial Monitoring Center should also be considered and, regardless of the decision made, the outcomes of such consideration should be documented and maintained.
- 2) Situation 2 suggests that the service offered or provided may pose a higher risk, although circumstances having impact on it are of positive nature within the given set of risks. In this case, again, for the purpose of determining risk exposure both the number and nature of higher risk criteria and the impact of the positive set of circumstances should be considered.
- 3) Situation 3 suggests that the service offered or provided poses medium risk, although certain circumstances are present, which may in future transform it into higher risk. In this case, it is important to establish enhanced ongoing monitoring over the service, as well as to conduct enhanced due diligence with the purpose of effectively controlling possible fluctuations in risk exposure.

4) Situation 4 suggests that the service offered or provided poses lower risk, and there is no material circumstance implying the possible presence of high risk criteria.

23. At that, if the service offered or provided comprises both higher and lower risk criteria, the aggregate risk exposure should be determined through assessing the nature and materiality of each risk criterion involved, as well as of the set of circumstances having impact on risk.

Chapter 9: General Rules for Client Due Diligence

24. Client due diligence or the principle “Know Your Client” is intended to ensure that realtors have adequate and comprehensive awareness of the real identity of their clients. This applies to identifying not only the clients, but also the authorized persons acting on behalf of them and the beneficial owners (if any).

25. Client due diligence should be conducted in each and every case of offering or providing a service, whether such service involves higher, medium, or lower risk. Client due diligence shall be required for both new and existing clients within the scope of services provided to them.

26. Article 15 of the Law defines the cases, the procedures, and the required minimum documentation for conducting client due diligence by realtors. Client due diligence shall comprise the following measures (Articles 15, 16 and 20 specify the requirements within the scope of each measure):

- 1) In accordance with Article 15 of the Law, obtain information on the identity (identification) of clients (including the authorized person acting on behalf of the client and the beneficial owner) and verifying the accuracy of the information obtained;
- 2) In accordance with Article 16 of the Law and Chapter 10 of this Guidance, perform ongoing monitoring of the business relationship (service);
- 3) In accordance with Article 15 of the Law and Chapters 11 and 12 of this Guidance, undertake measures based on risk-based approach for client due diligence.

27. At that, measures specified by Sub-Clause 1, Clause 26 of this Guidance shall be undertaken by realtors before providing services to clients. In exceptional circumstances, when the ML/TF risk is effectively prevented, and where it is essential not to impair the normal course of services provided to clients, measures towards obtaining information on the identity of the client and verification of such information may be undertaken after the service is actually provided, within a reasonable timeframe of not more than seven days.

Chapter 10: Ongoing Monitoring of Business Relationship (Service)

28. An essential constituent of client due diligence is the ongoing monitoring of clients and their business profile in the whole course of business relationships (services) provided by realtors, so as to form a complete and clear understanding of the purpose and the expected nature of the services provided. For this purpose, depending on the ML/TF risk exposure of the service

provided by realtors, the following measures shall be undertaken by them during the whole course of providing the service:

- 1) Verify the interconnection between transactions carried out within the scope of the service provided, detect possible schemes for these connections, as well as determine the objective of the transactions;
 - 2) Verify whether the nature of the transactions is commensurate to the type of business activities of the client;
 - 3) Check the categories, periodicity, and chronology of transactions carried out in a standard unit of time;
 - 4) Verify possible interrelations between the parties of transactions, the authorized persons, as well as the beneficial owners;
 - 5) Verify the existence of transactions by means of which clients pursue to avoid being reported to the Financial Monitoring Center by reporting entities;
 - 6) Obtain possibly complete information, as necessary, on the sources of income and (or) wealth of clients, and on the changes thereof;
 - 7) Compare the sources, turnover, and amounts of funds of the client subject to different transactions;
 - 8) Assess possible ML/TF risks in services offered or provided, by means of comparison with the criteria and typologies of suspicious transactions and business relationships.
29. Information obtained within the scope of conducted client due diligence (including enhanced and simplified due diligence) should be updated by realtors at a periodicity set by them, but not less than once a year, to ensure that it is up-to-date and relevant.

Chapter 11: Enhanced Client Due Diligence

30. In case the service offered or provided poses higher risk, realtors should, in addition to client due diligence measures prescribed under Chapter 9 of this Guidance, conduct enhanced client due diligence.

- 1) Enhanced client due diligence should include the following measures:
 - a. Obtain senior management approval before establishing and for continuing business relationships with such clients, as well as in cases when later on it is found out that clients and (or) the beneficial owners pose higher risk, or that the transactions or business relationships comprise such criteria;
 - b. Undertake necessary actions for verifying the source of income and (or) wealth of clients;
 - c. Scrutinize, record in writing, and maintain the grounds and conditions for the following transactions, so as to permit reconstruction of transaction details in future and, if necessary, dissemination of those to authorized bodies. Such transactions include:

- All complex and unusually large transactions, as well as unusual patterns of transactions with no apparent economic or legitimate purpose;
 - Transactions involving persons residing (located) in foreign countries or territories, where international requirements for combating money laundering and terrorism financing are absent or ineffectively implemented;
- d. Conduct enhanced ongoing monitoring of business relationships.
- 2) Enhanced client due diligence may include the following measures:
- a. Scrutinize the required documents (information), stipulated in case of offering and providing services, in a more comprehensive and thorough manner;
 - b. Make requests to authorized government bodies with the purpose of verifying the accuracy of information on clients, transactions with and services provided to them.
31. By means of enhanced client due diligence, realtors should obtain reasonable clarifications and explanations, so as to form a complete and clear understanding of the clients and the services offered or provided in relation to them.

Chapter 12: Simplified Client Due Diligence

32. In case of lower risk criteria, realtors may perform simplified client due diligence.
33. Simplified client due diligence shall be the limited implementation of client due diligence measures performed by realtors, whereby the following information shall be obtained as part of the identification and verification of identity:
- 1) For natural persons - forename, surname and identification document information;
 - 2) For legal persons – company name and state registration certificate number;
 - 3) For government bodies and local self-government bodies - name.

Chapter 13: Minimal Requirements for Recording and Maintaining Information

34. Realtors should record and maintain the information specified under Chapters 9-12 of this Guidance in a manner sufficient to permit reconstruction of individual transactions so as to provide, if necessary, procedural evidence.
35. Information may be maintained in documentary form, on computers, or other electronic means.
36. Realtors should ensure the security and secrecy of the information recorded and maintained, and should prevent it from unauthorized use or control.
37. Realtors should maintain the information specified under Article 20 of the Law, including the process of review (conducted analysis) for recognizing a transaction or business relationship as suspicious as specified under Clause 42 of this Guidance.

Chapter 14: Obligation in Relation to Suspicious Transaction or Business Relationship

38. From the moment of recognizing a transaction or business relationship as suspicious, realtors shall be obligated to file a suspicious transaction or business relationship report with the Financial Monitoring Center.

39. To recognize a transaction or a business relationship as suspicious, realtors should consider the criteria and (or) typologies of suspicious transactions or business relationships.

40. Legislative requirements in relation to suspicious transaction or business relationship reports are specified:

- 1) Under Articles 4-7 of the Law establishing that realtors shall be obligated to file a report with the Financial Monitoring Center in case of a suspicious transaction or business relationship;
- 2) Under Decision No15-N, of January 27, 2009 of the Board of the Central Bank of the Republic of Armenia establishing the Form No 024 for reporting suspicious transaction or business relationship by realtors, the rules and deadlines for its submission, as well as the rules for the registration of realtors,
- 3) Under Decision No1/886A, of September 3, 2008 of the Chairman of the Central Bank of the Republic of Armenia defining suspicious transaction criteria for all reporting entities, including realtors.

41. Realtors may also recognize a transaction or business relationship as suspicious, when such suspicion does not arise from any specific criteria and (or) typology of a suspicious transaction or business relationship, but its logic or pattern (dynamics) of implementation give the grounds to suspect that it is being carried out or established for the purpose of money laundering or terrorism financing.

42. In the presence of a criteria or typology of suspicious transaction or business relationship, as well as in the cases specified under Clause 41 of this Guidance, realtors should consider recognizing the transaction or business relationship as suspicious. If, due to such consideration, the transaction or business relationship is not recognized as suspicious, the process of review (conducted analysis) and the findings shall be documented and maintained in the manner and timeframe established by the Law and this Guidance.

ANNEX 25 - GUIDANCE FOR ENTITIES ORGANIZING GAMES OF CHANCE AND LOTTERIES AND CASINOS, INCLUDING ENTITIES ORGANISING ONLINE GAMES OF CHANCE, ON MINIMAL REQUIREMENTS FOR ASSESSING AND PREVENTING MONEY LAUNDERING AND TERRORISM FINANCING RISKS

**Approved by the Decision of the
Chairman of the Central Bank of the
Republic of Armenia, No 1/877 - A of August 6, 2010**

Introduction

1. This Guidance is presented based on Part 2, Article 11 of the Republic of Armenia Law on Combating Money Laundering and Terrorism Financing (hereinafter referred to as the Law) and is applicable to reporting entities such as Entities Organizing Games of Chance and Lotteries and Casinos, Including Entities Organizing Online Games of Chance (hereinafter referred to as reporting entities) as defined by Article 3 of the Law. The Guidance presents specific criteria of money laundering and terrorism financing (hereinafter also referred to as ML/TF) risks inherent to reporting entities, and the prevention mechanisms thereof.
2. The purposes of identifying and assessing ML/TF inherent risks and taking commensurate preventive measures by reporting entities are the following:
 - 4) The mechanisms prescribed by the Guidance would enable reporting entities to discern their higher risk clients and to take actions which would not impede their own activities aimed at making profit on one hand and would prevent possible risks arising from such clients on the other hand.
 - 5) Reporting entities would not impose unnecessarily restrictive rules upon all their clients while providing for those rules for higher risk clients and services only.
 - 6) Reporting entities would use their resources more efficiently for the purpose of deterring the entrance of criminal persons and preventing the turnover of criminal proceeds.
 - 7) Reporting entities would be safeguarded from possible future allegations of being involved in or facilitating different money laundering schemes, with the reasoning that they have effective systems in place for assessing and preventing ML/TF risks.
3. The Guidance also defines a comprehensive set of measures for reporting entities, which, when realized, would ensure compliance of their practices with requirements of the Law.
4. Concepts referred to in the Guidance are used in accordance with the concepts and formulations defined by the Law.

Section 1: Risks

Chapter 1: Importance of Categorizing and Managing Risks

5. ML/TF risks faced by reporting entities vary depending on many factors including the types of gambling offered, location and volumes of business, size of premises that are place for organizing games, payment methods accepted from clients, types of clients (regular clients, passing trade such as casual tourists or casino tours, etc.). The minimal comprehensive set of risks and their prevention mechanisms are defined by the Law.

6. Reporting entities should precisely identify the ML/TF risks and their prevention measures, which may be relevant in the course of their activities. Concurrently, every practical case or situation may give rise to new risks; therefore, the prevention measures must be dynamically developing ones.

7. ML/TF risks faced by reporting entities are classified into country or geographic, client, and service risk categories (for the purposes of this Guidance, the concept of service corresponds to that of business relationship as defined by the Law). These risk categories should not be considered separately, in isolation from one another, as for a certain category of risk can lead to the emergence of another category of risk, while, besides that, several categories of possible risks may simultaneously be present as well.

8. Based on own knowledge and experience, reporting entities should be able to identify existent ML/TF risks, assess each one of them and aggregate a comprehensive risk assessment for the same client or service.

9. Different categories of risks are presented under this Guidance with the following purposes:

- 1) To illustrate a minimal set of risks and, based on that, propose a model package of risk prevention measures;
- 2) To precisely identify ML/TF risks inherent to reporting entities by means of evaluating risks specified under the Guidance from the standpoint of their own practices.

Chapter 2: Country or Geographic Risk

10. There is no research conducted by any international organization that would designate a particular country or geographic area as undoubtedly and unconditionally presenting higher ML/TF risk for reporting entities. Nevertheless, the following countries and territories are considered to pose higher risk in terms of ML/TF:

- 1) Countries and territories subject to sanctions, embargoes, or similar restrictive measures issued by the UN²⁶;

²⁶ The FMC official web-site contains links to documents issued by the UN Security Council Sanctions Committee (www.cba.am/Financial_Monitoring_Center). Documents are available at www.un.org/sc/committees.

- 2) Countries and territories publicized by the FATF and FATF-style regional bodies as lacking or having inefficient AML/CFT systems²⁷.
- 3) Countries and territories publicized by international structures as having significant levels of corruption²⁸.
- 4) Countries and territories included in the list of off-shore jurisdictions as approved by the Central Bank of the Republic of Armenia²⁹.

11. Reporting entities should consider the above-listed countries and territories as posing higher risk if clients or beneficial owners are residing or located therein.

12. The factual location (where transactions are carried out) of clients may also pose higher risk for entities organizing online games of chance.

13. Besides the above, reporting entities may, based on own experience and practices, classify/consider any country or geographic area as posing higher risk, even if it is not listed under the above-specified criteria.

Chapter 3: Client Risk

14. Every reporting entity should have a clear understanding of which category of clients or which particular client poses higher ML/TF risk. In this sense, clients posing higher risk include:

- 9) Politically exposed persons³⁰;
- 2) High spenders that purchase tokens, make stakes and take winnings (for an amount exceeding 1 million drams)³¹;
- 3) Disproportionate spenders³²;

²⁷ The FMC official web-site contains links to FATF and MONEYVAL publications ([www.cba.am/Financial Monitoring Center](http://www.cba.am/Financial_Monitoring_Center)). The publications are available at www.fatf-gafi.org, www.coe.int/moneyval.

²⁸ See, for example, at www.transparency.org. The FMC official web-site contains links to data issued by Transparency International ([www.cba.am/Financial Monitoring Center](http://www.cba.am/Financial_Monitoring_Center)).

²⁹ See Republic of Armenia Central Bank Board Decision No 28, of July 28, 2009.

³⁰ The definition of politically exposed persons is stipulated by the Law, while relevant information can be found from various public sources, such as the search engine of www.google.am, the official web-site of the US Central Intelligence Agency (www.cia.gov/library/publications/the-world-factbook), web-sites of relevant governmental bodies of different countries, etc. Besides these, there are also different paid information databases (e.g. World-Check, Factiva, Accuity), which provide most comprehensive information on politically exposed persons. The FMC official web-site contains links to the stated information resources ([www.cba.am/Financial Monitoring Center](http://www.cba.am/Financial_Monitoring_Center)).

³¹ The amount of tokens (lotteries), gambling and winning is relative and is derived from the average amount of turnover in Armenia or the current institution.

³² As a result of client due diligence conducted by reporting entities, the information obtained on the business profile of the customer (including the sources of income and wealth) may provide grounds for assessing the proportionality of client spending.

- 4) Clients that spend unequally larger amounts on secondary services (refreshments, food, show tickets, entertainment) provided by reporting entities as compared to spending on lotteries or games of chance;
- 5) Casual clients³³;
- 6) Clients convicted for willfully committed crimes, if this circumstance becomes known to the reporting entity in the course of conducting professional activities;
- 7) Clients acting for the benefit or on behalf of other parties³⁴.

Chapter 4: Service Risk

15. Services posing higher risk are:

- 1) Online games of chance and lotteries;
- 2) Live games of chance.

Chapter 5: Lower Risk Criteria

16. Reporting entities can consider only the following circumstances as characterized by lower risk criteria (except for the clients residing or located in countries and territories lacking or having inefficient AML/CFT systems):

- 1) Regular clients with proportionate and legitimate sources of income (wealth) and positive business reputation;
- 2) Games of chance on automated slot machines that accept stakes of not more than 10000 drams, and provide for one-time winnings of not more than 20000 drams.
- 3) Lotteries with low-value winnings (not more than 10000 drams),

Chapter 6: Variables That May Impact Risk Criteria

17. ML/TF risks inherent to practices of reporting entities and the resources required for their mitigation are all dependant on the volumes, sphere, experience and other conditions of their activities. Therefore, every reporting entity should precisely identify the circumstances having impact on the formation of ML/TF risk criteria in the course of its practices. Typical examples of such circumstances are:

- 1) Nature (one-time or recurrent), duration, regularity, and periodicity of services offered or provided;
- 2) Rating and business reputation of the client;

³³ This group (e.g. tourists) includes casual clients of the current institution.

³⁴ e.g. when it is apparent that stakes are made on behalf or for the benefit of a person but the actual gambler is a different person.

- 3) Client residency and, in case of foreign clients, the nature of their relation with the Republic of Armenia;
- 4) Circumstances related to introducing the client (whether the client has been recommended to the reporting entity by another reputable or familiar party, or has applied without prior appointment);
- 5) Clients acting in concert or in separate;
- 6) Presence of more than one higher or lower risk criterion within the service provided to the client;
- 7) Payment methods accepted from clients and offered to clients (cash or non-cash);
- 8) Reporting entity is part of a network company or operates by its own;
- 9) Reporting entity casino or an entity organizing games of chance is providing services (e.g. hotels, entertainment) other than gambling services;
- 10) Management bodies or technical equipments of reporting entities are located in the Republic of Armenia or abroad (e.g. servers of internet operators are located in countries other than the business location of the reporting entity);
- 11) Turnover volumes, number of employees of reporting entities and their experience levels;
- 12) Size of premises where the reporting entity is located/operates;
- 13) Provision of "VIP" services and their conditions.

Section 2: Risk Prevention Measures

Chapter 7: Internal Monitoring Function for Prevention of Risk and "Fit and Proper" Rules

18. For the purpose of effective prevention of ML/TF risks specified under Section 1 of this Guidance, reporting entities should introduce an internal monitoring function. At that, in order to appropriately realize this function, in accordance with Article 22 of the Law, reporting entities shall be obligated to have an internal monitoring unit or an employee responsible for dealing with the prevention of ML/TF, or otherwise outsource this function to relevant specialized entities (hereinafter referred to as internal monitoring unit).

19. The unit performing internal monitoring functions of a reporting entity should at least undertake the following measures:

- 1) Develop AML/CFT internal legal acts (in case of having more than 10 employees); present proposals on enhancing effectiveness of such acts;
- 2) Categorize clients and services provided to them in terms of ML/TF risk exposure in accordance with the Law, this Guidance, and internal legal acts of the reporting entity; build up awareness among employees of the reporting entity about specific categories of risks, and higher risk clients and services;
- 3) Provide for regulation and effectiveness of client due diligence processes, including enhanced and simplified due diligence, as well as for the ongoing monitoring of clients

- and of the business profile thereof, information recording, maintenance, and updating processes;
- 4) Conduct analysis in relation to recognizing a transaction or business relationship (purchase of tokens or lotteries, stakes and winnings) as suspicious;
 - 5) Make the final decision with regard to recognizing a transaction or business relationship as suspicious, to rejecting or suspending them, as well as to freezing of funds or other assets associated to terrorism;
 - 6) Ensure the filing of suspicious transaction or business relationship reports with the Financial Monitoring Center of the Central Bank of the Republic of Armenia (hereinafter referred to as the Financial Monitoring Center);
 - 7) Undertake other measures of risk prevention as prescribed under this Section.
20. The structural unit of reporting entities performing the functions of internal monitoring should have direct and timely access to any document or information in relation to services provided by reporting entities.
21. Reporting entities should strictly follow the "Fit and Proper" rules and, for this purpose, should:
- 1) Verify the biography of its owners that are natural persons, senior managers and beneficial owners.
 - 2) Deter (prohibit) any formation of ownership, management connections with persons that have conviction records in biographic data or when their possible connections of criminal nature are revealed.

Chapter 8: Risk Assessment Methods

22. Before providing services to clients and during the entire duration of regular services, reporting entities should assess the aggregate ML/TF risk exposure in relation to them. In the course of assessing client and service risk, the following matrix is recommended as a guide in order to consider risk criteria and circumstances having impact on them, as specified under Section 1 of this Guidance.

	<i>Negative Set of Circumstances Having Impact on Risk</i>	<i>Positive Set of Circumstances Having Impact on Risk</i>
<i>Higher Risk Criteria Stance</i>	1	2
<i>Lower Risk Criteria Stance</i>	3	4

- 1) Situation 1 suggests that the service offered or provided poses higher risk. For the purpose of determining risk exposure, it is also important to consider what the higher risk criteria are and how many of such criteria are present. In this case, the question of filing a suspicious transaction or business relationship report with the Financial Monitoring Center should also be considered and, regardless of the decision made, the outcomes of such consideration should be documented and maintained.
- 2) Situation 2 suggests that the service offered or provided may pose a higher risk, although circumstances having impact on it are of positive nature within the given set of risks. In this case, again, for the purpose of determining risk exposure both the number and nature of higher risk criteria and the impact of the positive set of circumstances should be considered.
- 3) Situation 3 suggests that the service offered or provided poses medium risk, although certain circumstances are present, which may in future transform it into higher risk. In this case, it is important to establish enhanced ongoing monitoring over the service, as well as to conduct enhanced due diligence with the purpose of effectively controlling possible fluctuations in risk exposure.
- 4) Situation 4 suggests that the service offered or provided poses lower risk, and there is no material circumstance implying the possible presence of high risk criteria.

23. At that, if the service offered or provided comprises both higher and lower risk criteria, the aggregate risk exposure should be determined through assessing the nature and materiality of each risk criterion involved, as well as of the set of circumstances having impact on risk.

Chapter 9: General Rules for Client Due Diligence

24. Client due diligence or the principle “Know Your Client” is intended to ensure that reporting entities have adequate and comprehensive awareness of the real identity of their clients.

25. Client due diligence should be conducted in each and every case of offering or providing a service, whether such service involves higher, medium, or lower risk. Client due diligence shall be required for both new and existing clients within the scope of services provided to them.

26. Article 15 of the Law defines the cases, the procedures, and the required minimum documentation for conducting client due diligence by reporting entities. Client due diligence shall comprise the following measures (Articles 15, 16 and 20 specify the requirements within the scope of each measure):

- 1) In accordance with Article 15 of the Law, obtain information on the identity (identification) of clients (including beneficial owner) and verifying the accuracy of the information obtained;
- 2) In accordance with Article 16 of the Law and Chapter 10 of this Guidance, perform ongoing monitoring of the business relationship (service);
- 3) In accordance with Article 15 of the Law and Chapters 11 and 12 of this Guidance, undertake measures based on risk-based approach for client due diligence.

27. At that, measures specified by Sub-Clause 1, Clause 26 of this Guidance shall be undertaken by reporting entities before providing services to clients. In exceptional circumstances, when the ML/TF risk is effectively prevented, and where it is essential not to impair the normal course of services provided to clients, measures towards obtaining information on the identity of the client and verification of such information may be undertaken after the service is actually provided, within a reasonable timeframe of not more than seven days.

Chapter 10: Ongoing Monitoring of Business Relationship (Service)

28. An essential constituent of client due diligence is the ongoing monitoring of clients and their business profile in the whole course of business relationships (services) provided by reporting entities, so as to form a complete and clear understanding of the purpose and the expected nature of the services provided. For this purpose, depending on the ML/TF risk exposure of the service provided by reporting entities, the following measures shall be undertaken by them during the whole course of providing the service:

- 1) Verify the interconnection between transactions carried out within the scope of the service provided, detect possible schemes for these connections, as well as determine the objective of the transactions;
- 2) Check the categories, periodicity, and chronology of transactions carried out in a standard unit of time;
- 3) Verify possible interrelations between the clients and beneficial owners;

- 4) Verify the existence of transactions by means of which clients pursue to avoid being reported to the Financial Monitoring Center by reporting entities;
 - 5) Obtain possibly complete information, as necessary, on the sources of income and (or) wealth of clients, and on the changes thereof;
 - 6) Compare the sources, turnover, and amounts of funds of the client subject to different transactions;
 - 7) Assess possible ML/TF risks in services offered or provided, by means of comparison with the criteria and typologies of suspicious transactions and business relationships.
29. Information obtained within the scope of conducted client due diligence (including enhanced and simplified due diligence) should be updated by reporting entities at a periodicity set by them, but not less than once a year, to ensure that it is up-to-date and relevant.

Chapter 11: Enhanced Client Due Diligence

30. In case the service offered or provided poses higher risk, reporting entities should, in addition to client due diligence measures prescribed under Chapter 9 of this Guidance, conduct enhanced client due diligence.

- 1) Enhanced client due diligence should include the following measures:
 - a. Obtain senior management approval before establishing and for continuing business relationships with such clients, as well as in cases when later on it is found out that clients and (or) the beneficial owners pose higher risk, or that the transactions or business relationships comprise such criteria;
 - b. Undertake necessary actions for verifying the source of income and (or) wealth of clients;
 - c. Scrutinize, record in writing, and maintain the grounds and conditions for the following transactions, so as to permit reconstruction of transaction details in future and, of necessary, dissemination of those to authorized bodies. Such transactions include:
 - All complex and unusually large transactions, as well as unusual patterns of transactions with no apparent economic or legitimate purpose;
 - Transactions involving persons residing (located) in foreign countries or territories, where international requirements for combating money laundering and terrorism financing are absent or ineffectively implemented;
 - d. Conduct enhanced ongoing monitoring of business relationships.
- 2) Enhanced client due diligence may include the following measures:
 - a. Scrutinize the required documents (information), stipulated in case of offering and providing services, in a more comprehensive and thorough manner;

- b. Make requests to authorized government bodies with the purpose of verifying the accuracy of information on clients, transactions with and services provided to them.

31. By means of enhanced client due diligence, reporting entities should obtain reasonable clarifications and explanations, so as to form a complete and clear understanding of the clients and the services offered or provided in relation to them.

Chapter 12: Simplified Client Due Diligence

32. In case of lower risk criteria, reporting entities may perform simplified client due diligence.

33. Simplified client due diligence shall be the limited implementation of client due diligence measures performed by reporting entities, whereby the following information shall be obtained as part of the identification and verification of identity:

- 1) Forename and surname;
- 2) Identification document information.

Chapter 13: Minimal Requirements for Recording and Maintaining Information

34. Reporting entities should record and maintain the information specified under Chapters 9-12 of this Guidance in a manner sufficient to permit reconstruction of individual transactions so as to provide, if necessary, procedural evidence.

35. Information may be maintained in documentary form, on computers, or other electronic means.

36. Reporting entities should ensure the security and secrecy of the information recorded and maintained, and should prevent it from unauthorized use or control.

37. Reporting entities should maintain the information specified under Article 20 of the Law, including the process of review (conducted analysis) for recognizing a transaction or business relationship as suspicious as specified under Clause 42 of this Guidance.

Chapter 14: Obligation in Relation to Suspicious Transaction or Business Relationship

38. From the moment of recognizing a transaction or business relationship as suspicious, reporting entities shall be obligated to file a suspicious transaction or business relationship report with the Financial Monitoring Center.

39. To recognize a transaction or a business relationship as suspicious, reporting entities should consider the criteria and (or) typologies of suspicious transactions or business relationships.

40. Legislative requirements in relation to suspicious transaction or business relationship reports are specified:

- 1) Under Articles 4-7 of the Law establishing that reporting entities shall be obligated to file a report with the Financial Monitoring Center in case of a suspicious transaction or business relationship;
- 2) Under Decisions No 234-N, 235-N of July 31, 2008 of the Board of the Central Bank of the Republic of Armenia establishing the Forms No 004 and 005 for reporting suspicious transaction or business relationship by reporting entities, the rules and deadlines for their submission, as well as the rules for the registration of reporting entities.
- 3) Under Decision No1/886A, of September 3, 2008 of the Chairman of the Central Bank of the Republic of Armenia defining suspicious transaction criteria for all reporting entities, including reporting entities.

41. Reporting entities may also recognize a transaction or business relationship as suspicious, when such suspicion does not arise from any specific criteria and (or) typology of a suspicious transaction or business relationship, but its logic or pattern (dynamics) of implementation give the grounds to suspect that it is being carried out or established for the purpose of money laundering or terrorism financing.

42. In the presence of a criteria or typology of suspicious transaction or business relationship, as well as in the cases specified under Clause 41 of this Guidance, reporting entities should consider recognizing the transaction or business relationship as suspicious. If, due to such consideration, the transaction or business relationship is not recognized as suspicious, the process of review (conducted analysis) and the findings shall be documented and maintained in the manner and timeframe established by the Law and this Guidance.

ANNEX 26 - GUIDANCE for ATTORNEYS, SOLE PRACTITIONER LAWYERS AND FIRMS PROVIDING LEGAL SERVICES ON MINIMAL REQUIREMENTS FOR ASSESSING AND PREVENTING MONEY LAUNDERING AND TERRORISM FINANCING RISKS

**Approved by the Decision of the
Chairman of the Central Bank of the
Republic of Armenia, No 1/878 - A of August 6, 2010**

Introduction

1. This Guidance is presented based on Part 2, Article 11 of the Republic of Armenia Law on Combating Money Laundering and Terrorism Financing (hereinafter referred to as the Law) and is applicable to reporting entities such as attorneys, sole practitioner lawyers and firms providing legal services (hereinafter referred to as legal professionals) as defined by Article 3 of the Law. The Guidance presents specific criteria of money laundering and terrorism financing (hereinafter also referred to as ML/TF) risks inherent to legal professionals, and the prevention mechanisms thereof.

2. The purposes of identifying and assessing ML/TF inherent risks and taking commensurate preventive measures by legal professionals are the following:

- 1) Legal professionals would safeguard their high rating and reputation in the view of the clients and the public, with the reasoning that in practice they are engaged exceptionally in legitimate activities.
- 2) The mechanisms prescribed by the Guidance would enable legal professionals to discern their higher risk clients and to take actions which would not impede their own activities aimed at making profit on one hand and would prevent possible risks arising from such clients on the other hand.
- 3) Legal professionals would be safeguarded from possible future allegations of being involved in or facilitating different money laundering schemes, with the reasoning that they have effective systems in place for assessing and preventing ML/TF risks.

3. The Guidance also defines a comprehensive set of measures for legal professionals, which, when realized, would ensure compliance of their practices with requirements of the Law. At that, as prescribed by the Law, provisions set forth under the Guidance are applicable to legal professionals only in terms of services involving the following transactions prepared or carried out for the client:

- 1) Buying and selling of real estate,
- 2) Managing of client money, securities or other assets,
- 3) Managing of bank and securities accounts,

- 4) Provision of funds or other assets for the establishment, operation, or management of legal persons,
- 5) Provision of services for the establishment, operation, or management of legal persons, as well as for the alienation (acquisition) of stocks (equities, shares and the like) in the statutory (equity and the like) capital of legal persons, or for the alienation (acquisition) of stock issues (stocks, shares and the like) of legal persons at a nominal or market value;
4. Concepts referred to in the Guidance are used in accordance with the concepts and formulations defined by the Law.

Section 1: Risks

Chapter 1: Importance of Categorizing and Managing Risks

5. ML/TF risks faced by legal professionals vary depending on many factors including the professional activity of legal professionals, the type and identity of clients, the nature of relationships with clients, and the methods for providing services (for the purposes of this Guidance, the concept of service corresponds to that of business relationship as defined by the Law). The minimal comprehensive set of risks and their prevention mechanisms are defined by the Law.
6. Legal professionals should precisely identify the ML/TF risks and their prevention measures, which may be relevant in the course of their activities. Concurrently, every practical case or situation may give rise to new risks; therefore, the prevention measures must be dynamically developing ones.
7. In comparison to, for example, financial institutions, the following reasons are behind the distinctiveness of ML/TF risk management by legal professionals:
 - 1) As part of their operations, financial institutions upon the instruction of customers manage their funds (attract deposits, make transfers, etc); hence, they have the objective to ensure that there is a reasonable and legitimate flow of funds in the course of providing such financial services. For the purpose of their practices, legal professionals have the objective to understand the true purpose behind the behavior of their clients, and the factual logic and legitimacy of the services offered or provided.
 - 2) Due to the large number of customers and the significant amount of funds under transactions, financial institutions exploit not only professional and human resources but also automated software systems for the purpose of preventing ML/TF risks. In practice, legal professionals exclusively rely on their own professional and personal skills.
8. Legal professionals may face higher or lower risk criteria.
9. Higher risk criteria, in turn, are classified into country or geographic, client, and transaction risk categories. These risk categories should not be considered separately, in isolation from one another, as for the presence of a higher risk criterion in one of the categories can lead to the presence of a higher risk criterion in another risk category or affect the possibility of the

emergence of such. Besides, the same service provided by a legal professional is possibly to simultaneously comprise more than one risk criterion pertaining to one or several risk categories.

10. Based on own knowledge and experience, legal professionals should be able to identify existent ML/TF risks, assess each one of them and aggregate a comprehensive risk assessment for the services offered or provided.

11. Different categories of risks are presented under this Guidance with the following purposes:

- 1) To illustrate a minimal set of risks and, based on that, propose a model package of risk prevention measures;
- 2) To precisely identify ML/TF risks inherent to legal professionals by means of evaluating risks specified under the Guidance from the standpoint of their own practices.

Chapter 2: Country or Geographic Risk

12. There is no research conducted by any international organization that would designate a particular country or geographic area as undoubtedly and unconditionally presenting higher ML/TF risk for legal professionals. Nevertheless, the following countries and territories are considered to pose higher risk in terms of ML/TF:

- 1) Countries and territories subject to sanctions, embargoes, or similar restrictive measures issued by the UN³⁵;
- 2) Countries and territories publicized by the FATF and FATF-style regional bodies as lacking or having inefficient AML/CFT systems³⁶.
- 3) Countries and territories publicized by international structures as having significant levels of corruption³⁷.
- 4) Countries and territories included in the list of off-shore jurisdictions as approved by the Central Bank of the Republic of Armenia³⁸.

13. Legal professionals should consider the above-listed countries and territories as posing higher risk if:

- 1) Clients, authorized persons, beneficial owners are residing or located in these countries and territories, or clients that have business relationships with them,
- 2) The source of income and (or) wealth of clients is in these countries or territories,
- 3) These countries and territories are the place for the conduction of the business relationship and (or) transaction.

³⁵ The FMC official web-site contains links to documents issued by the UN Security Council Sanctions Committee (www.cba.am/Financial_Monitoring_Center). Documents are available at www.un.org/sc/committees.

³⁶ The FMC official web-site contains links to FATF and MONEYVAL publications (www.cba.am/Financial_Monitoring_Center). The publications are available at www.fatf-gafi.org, www.coe.int/moneyval.

³⁷ See, for example, at www.transparency.org. The FMC official web-site contains links to data issued by Transparency International (www.cba.am/Financial_Monitoring_Center).

³⁸ See Republic of Armenia Central Bank Board Decision No 28, of July 28, 2009.

14. Besides the above, legal professionals may, based on own experience and practices, classify/consider any country or geographic area as posing higher risk, even if it is not listed under the above-specified criteria.

Chapter 3: Client Risk

15. Every legal professional should have a clear understanding of which category of clients or which particular client poses higher ML/TF risk. In this sense, clients posing higher risk include:

- 1) Politically exposed persons³⁹;
- 2) Corporate clients with unnecessarily complex control structure of management bodies or beneficial owners that are impossible to identify;
- 3) Clients that are cash intensive businesses (e.g. casinos, gas stations, hotels, etc.);
- 4) Resident or non-resident non-profit organizations (including charities), where there is:
 - a. No apparent corporate structure resulting in considerable divergence from the requirements specified under the applicable legislation; and (or)
 - b. No authorized supervisory body entitled to examine financial and business operations of these organizations and impose responsibility measures for the violations disclosed;
- 5) Clients convicted for willfully committed crimes, if this circumstance becomes known to the legal professional in the course of conducting professional activities;
- 6) Clients having numerously changed the address of their permanent living (registration), location, or business;
- 7) Legal persons having factually conducted no activity during a considerable period of time;
- 8) Shell companies having state registration but no factual address of location or any activity conducted.

Chapter 4: Transaction Risk

16. Certain transactions (subjects of legal advisory) conducted by legal professionals for their clients may pose higher ML/TF risks. These include cases when:

³⁹ The definition of politically exposed persons is stipulated by the Law, while relevant information can be found from various public sources, such as the search engine of www.google.am, the official web-site of the US Central Intelligence Agency (www.cia.gov/library/publications/the-world-factbook), web-sites of relevant governmental bodies of different countries, etc. Besides these, there are also different paid information databases (e.g. World-Check, Factiva, Accuity), which provide most comprehensive information on politically exposed persons. The FMC official web-site contains links to the stated information resources (www.cba.am/Financial Monitoring Center).

- 1) A transaction is offered to carry out with the purpose of concealing beneficial owners of the client (e.g. arranging a creation contract of a legal person, where the beneficial owner acts in a mediated way – by means of being the founder of the founding legal person);
- 2) A transaction is offered, where the price is apparently lower or higher than the real/market price of the subject of transaction (e.g. arranging a real estate buying and selling contract at an apparently low price);
- 3) Payment to legal professionals for completing a transaction, or payment to clients against a transaction, is unreasonably made by a party un-associated with the client;
- 4) Corporate clients provide for making payments to legal professionals in cash;
- 5) Clients provide apparently fake or incomplete information about the real objectives, nature, and subject of the transactions carried out;
- 6) Clients promise to pay unreasonably high fees for transactions carried out, except for the cases of wealthy clients promising bonuses for successful completion of transactions;
- 7) Transactions offered or carried out are apparently not commensurate to the business profile of the client (e.g. an individual entrepreneur providing tourism services requests advisory on contracts for importing precious stones);
- 8) A transaction is offered, where parties (to be) involved (would) maintain their anonymity (e.g. an offer is placed for a service to establish a company with nominal founders and directors in an off-shore jurisdiction).

Chapter 5: Lower Risk Criteria

17. Legal professionals can consider only the following clients as characterized by lower risk criteria (except for the clients residing or located in countries and territories lacking or having inefficient AML/CFT systems):

- 1) Financial institutions effectively supervised in terms of combating money laundering and terrorism financing,
- 2) Governmental bodies,
- 3) Local self-government bodies,
- 4) State-owned non commercial organizations,
- 5) Public administration institutions.

Chapter 6: Variables That May Impact Risk Criteria

18. ML/TF risks inherent to practices of legal professionals and resources in place for their mitigation are all dependant on the size, sphere, expertise and other conditions of their activities. For example, ML/TF risks and mitigation resources for a sole practitioner attorney will be different from that of a large firm providing legal advisory services. Therefore, every legal professional should precisely identify the circumstances having impact on the formation of ML/TF risk criteria in the course of his practices. Typical examples of such circumstances are:

- 1) Nature (one-time or recurrent), duration, regularity, and periodicity of services offered or provided;
- 2) Robustness of the legal regime (e.g. licensing, registration rules) applicable to the clients,
- 3) Rating and business reputation of the client;
- 4) Nature of the legal advisory services (non- or face to face communication);
- 5) Client residency and, in case of foreign clients, the nature of their relation with the Republic of Armenia;
- 6) Circumstances related to introducing the client (whether the client has been recommended to the legal professional by another reputable or familiar party, or has applied without prior appointment);
- 7) Presence of more than one higher or lower risk criterion within the service provided to the client.

Section 2: Risk Prevention Measures

Chapter 7: Internal Monitoring Function for Prevention of Risk

19. For the purpose of effective prevention of ML/TF risks specified under Section 1 of this Guidance, legal professionals should introduce an internal monitoring function. At that, in order to appropriately realize this function, in accordance with Article 22 of the Law, legal professionals shall be obligated to have an internal monitoring unit or an employee responsible for dealing with the prevention of ML/TF, or otherwise outsource this function to relevant specialized entities (hereinafter referred to as internal monitoring unit).

20. Taking into consideration that the size of activities and human resources of legal professionals are significantly inferior to the relevant characteristics of financial institutions and that, in addition, there are profound differences in terms of activities and human resources amongst legal professionals (from a sole practitioner attorney to a large firm providing legal advisory services), Article 22 of the Law shall be applicable to legal professionals with the following differences:

- 1) In case of sole practitioner lawyers, the internal monitoring function of ML/TF prevention should be performed by the sole practitioner lawyers themselves;
- 2) In case there is specialized staff available, the function may be assigned to an individual employee or a structural unit. In this case, the autonomy and direct accountability of the internal monitoring unit to the senior management of the legal professional should be ensured.

21. The unit performing internal monitoring functions of a legal professional should at least undertake the following measures:

- 1) Develop AML/CFT internal legal acts (in case of having more than 10 employees); present proposals on enhancing effectiveness of such acts;
- 2) Categorize clients and services provided to them in terms of ML/TF risk exposure in accordance with the Law, this Guidance, and internal legal acts of the legal professional; build up awareness among employees of the legal professional about specific categories of risks, and higher risk clients and services;

- 3) Provide for regulation and effectiveness of client due diligence processes, including enhanced and simplified due diligence, as well as for the ongoing monitoring of clients and of the business profile thereof, information recording, maintenance, and updating processes;
 - 4) Conduct analysis in relation to recognizing a transaction or business relationship as suspicious;
 - 5) Make the final decision with regard to recognizing a transaction or business relationship as suspicious, to rejecting or suspending them, as well as to freezing of funds or other assets associated to terrorism;
 - 6) Ensure the filing of suspicious transaction or business relationship reports with the Financial Monitoring Center of the Central Bank of the Republic of Armenia (hereinafter referred to as the Financial Monitoring Center);
 - 7) Undertake other measures of risk prevention as prescribed under this Section.
22. The structural unit of legal professionals performing the functions of internal monitoring should have direct and timely access to any document or information in relation to services provided by legal professionals.

Chapter 8: Risk Assessment Methods

23. Before providing services to clients and during the entire duration of in-progress contractual services, legal professionals should assess the aggregate ML/TF risk exposure in relation to them. In the course of assessing client and transaction risk, the following matrix is recommended as a guide in order to consider risk criteria and circumstances having impact on them, as specified under Section 1 of this Guidance.

	<i>Negative Set of Circumstances Having Impact on Risk</i>	<i>Positive Set of Circumstances Having Impact on Risk</i>
<i>Higher Risk Criteria Stance</i>	1	2
<i>Lower Risk Criteria Stance</i>	3	4

- 1) Situation 1 suggests that the service offered or provided poses higher risk. For the purpose of determining risk exposure, it is also important to consider what the higher risk

criteria are and how many of such criteria are present. In this case, the question of filing a suspicious transaction or business relationship report with the Financial Monitoring Center should also be considered and, regardless of the decision made, the outcomes of such consideration should be documented and maintained.

- 2) Situation 2 suggests that the service offered or provided may pose a higher risk, although circumstances having impact on it are of positive nature within the given set of risks. In this case, again, for the purpose of determining risk exposure both the number and nature of higher risk criteria and the impact of the positive set of circumstances should be considered.
- 3) Situation 3 suggests that the service offered or provided poses medium risk, although certain circumstances are present, which may in future transform it into higher risk. In this case, it is important to establish enhanced ongoing monitoring over the service, as well as to conduct enhanced due diligence with the purpose of effectively controlling possible fluctuations in risk exposure.
- 4) Situation 4 suggests that the service offered or provided poses lower risk, and there is no material circumstance implying the possible presence of high risk criteria.

24. At that, if the service offered or provided comprises both higher and lower risk criteria, the aggregate risk exposure should be determined through assessing the nature and materiality of each risk criterion involved, as well as of the set of circumstances having impact on risk.

Chapter 9: General Rules for Client Due Diligence

25. Client due diligence or the principle “Know Your Client” is intended to ensure that legal professionals have adequate and comprehensive awareness of the real identity of their clients. This applies to identifying not only the clients, but also the authorized persons acting on behalf of them and the beneficial owners (if any).

26. Client due diligence should be conducted in each and every case of offering or providing a service, whether such service involves higher, medium, or lower risk. Client due diligence shall be required for both new and existing clients within the scope of services provided to them.

27. Article 15 of the Law defines the cases, the procedures, and the required minimum documentation for conducting client due diligence by legal professionals. Client due diligence shall comprise the following measures (Articles 15, 16 and 20 specify the requirements within the scope of each measure):

- 1) In accordance with Article 15 of the Law, obtain information on the identity (identification) of clients (including the authorized person acting on behalf of the client and the beneficial owner) and verifying the accuracy of the information obtained;
- 2) In accordance with Article 16 of the Law and Chapter 10 of this Guidance, perform ongoing monitoring of the business relationship (service);
- 3) In accordance with Article 15 of the Law and Chapters 11 and 12 of this Guidance, undertake measures based on risk-based approach for client due diligence.

28. At that, measures specified by Sub-Clause 1, Clause 27 of this Guidance shall be undertaken by legal professionals before providing services to clients. In exceptional circumstances, when the ML/TF risk is effectively prevented, and where it is essential not to impair the normal course of services provided to clients, measures towards obtaining information on the identity of the client and verification of such information may be undertaken after the service is actually provided, within a reasonable timeframe of not more than seven days.

Chapter 10: Ongoing Monitoring of Business Relationship (Service)

29. An essential constituent of client due diligence is the ongoing monitoring of clients and their business profile in the whole course of business relationships (services) provided by legal professionals, so as to form a complete and clear understanding of the purpose and the expected nature of the services provided. For this purpose, depending on the ML/TF risk exposure of the service provided by legal professionals, the following measures shall be undertaken by them during the whole course of providing the service:

- 1) Verify the interconnection between transactions carried out within the scope of the service provided, detect possible schemes for these connections, as well as determine the objective of the transactions;
- 2) Verify whether the nature of the transactions is commensurate to the type of business activities of the client;
- 3) Check the categories, periodicity, and chronology of transactions carried out in a standard unit of time;
- 4) Verify possible interrelations between the parties of transactions, the authorized persons, as well as the beneficial owners;
- 5) Verify the existence of transactions by means of which clients pursue to avoid being reported to the Financial Monitoring Center by reporting entities;
- 6) Obtain possibly complete information, as necessary, on the sources of income and (or) wealth of clients, and on the changes thereof;
- 7) Compare the sources, turnover, and amounts of funds of the client subject to different transactions;
- 8) Assess possible ML/TF risks in services offered or provided, by means of comparison with the criteria and typologies of suspicious transactions and business relationships.

30. Information obtained within the scope of conducted client due diligence (including enhanced and simplified due diligence) should be updated by legal professionals at a periodicity set by them, but not less than once a year, to ensure that it is up-to-date and relevant.

Chapter 11: Enhanced Client Due Diligence

31. In case the service offered or provided poses higher risk, legal professionals should, in addition to client due diligence measures prescribed under Chapter 9 of this Guidance, conduct enhanced client due diligence.

- 1) Enhanced client due diligence should include the following measures:
 - a. Obtain senior management approval before establishing and for continuing business relationships with such clients, as well as in cases when later on it is found out that clients and (or) the beneficial owners pose higher risk, or that the transactions or business relationships comprise such criteria;
 - b. Undertake necessary actions for verifying the source of income and (or) wealth of clients;
 - c. Scrutinize, record in writing, and maintain the grounds and conditions for the following transactions, so as to permit reconstruction of transaction details in future and, of necessary, dissemination of those to authorized bodies. Such transactions include:
 - All complex and unusually large transactions, as well as unusual patterns of transactions with no apparent economic or legitimate purpose;
 - Transactions involving persons residing (located) in foreign countries or territories, where international requirements for combating money laundering and terrorism financing are absent or ineffectively implemented;
 - d. Conduct enhanced ongoing monitoring of business relationships.
- 2) Enhanced client due diligence may include the following measures:
 - a. Scrutinize the required documents (information), stipulated in case of offering and providing services, in a more comprehensive and thorough manner;
 - b. Make requests to authorized government bodies with the purpose of verifying the accuracy of information on clients, transactions with and services provided to them.

32. By means of enhanced client due diligence, legal professionals should obtain reasonable clarifications and explanations, so as to form a complete and clear understanding of the clients and the services offered or provided in relation to them.

Chapter 12: Simplified Client Due Diligence

33. In case of lower risk criteria, legal professionals may perform simplified client due diligence.

34. Simplified client due diligence shall be the limited implementation of client due diligence measures performed by legal professionals, whereby the following information shall be obtained as part of the identification and verification of identity:

1. For natural persons - forename, surname and identification document information;
2. For legal persons – company name and state registration certificate number;
3. For government bodies and local self-government bodies - name.

Chapter 13: Minimal Requirements for Recording and Maintaining Information

35. Legal professionals should record and maintain the information specified under Chapters 9-12 of this Guidance in a manner sufficient to permit reconstruction of individual transactions so as to provide, if necessary, procedural evidence.

36. Information may be maintained in documentary form, on computers, or other electronic means.

37. Legal professionals should ensure the security and secrecy of the information recorded and maintained, and should prevent it from unauthorized use or control.

38. Legal professionals should maintain the information specified under Article 20 of the Law, including the process of review (conducted analysis) for recognizing a transaction or business relationship as suspicious as specified under Clause 43 of this Guidance.

Chapter 14: Obligation in Relation to Suspicious Transaction or Business Relationship

39. From the moment of recognizing a transaction or business relationship as suspicious, legal professionals shall be obligated to file a suspicious transaction or business relationship report with the Financial Monitoring Center.

40. To recognize a transaction or a business relationship as suspicious, legal professionals should consider the criteria and (or) typologies of suspicious transactions or business relationships.

41. Legislative requirements in relation to suspicious transaction or business relationship reports are specified:

- 1) Under Articles 4-7 of the Law establishing that legal professionals shall be obligated to file a report with the Financial Monitoring Center in case of a suspicious transaction or business relationship;
- 2) Under Decision No16-N, of January 27, 2009 of the Board of the Central Bank of the Republic of Armenia establishing the Form No 020 for reporting suspicious transaction or business relationship by legal professionals, the rules and deadlines for its submission, as well as the rules for the registration of legal professionals,
- 3) Under Decision No1/886A, of September 3, 2008 of the Chairman of the Central Bank of the Republic of Armenia defining suspicious transaction criteria for all reporting entities, including legal professionals.

42. Legal professionals may also recognize a transaction or business relationship as suspicious, when such suspicion does not arise from any specific criteria and (or) typology of a suspicious

transaction or business relationship, but its logic or pattern (dynamics) of implementation give the grounds to suspect that it is being carried out or established for the purpose of money laundering or terrorism financing.

43. In the presence of a criteria or typology of suspicious transaction or business relationship, as well as in the cases specified under Clause 42 of this Guidance, legal professionals should consider recognizing the transaction or business relationship as suspicious. If, due to such consideration, the transaction or business relationship is not recognized as suspicious, the process of review (conducted analysis) and the findings shall be documented and maintained in the manner and timeframe established by the Law and this Guidance.

ANNEX 27 – EXTRACT FROM THE DECISION OF THE CHAIRMAN OF THE REPUBLIC OF ARMENIA CENTRAL BANK No 1-1315L OF OCTOBER 19, 2009 (ON ON-SITE INSPECTIONS IN BANKS)

6.9. Combating Money Laundering and Terrorism Financing

6.9.1. Introduction

In the capacity of the Authorized Body for combating money laundering and terrorism financing (hereinafter also referred to as ML/FT), the Central Bank places special emphasis on the banks to take measures in the manner established by law and other legal statutes for recognizing and preventing suspicious transactions (business relationships) of their customers or third parties.

The Republic of Armenia Law on Combating Money Laundering and Terrorism Financing (having entered into force on August 31, 2008) established the legal mechanisms to counter money laundering and terrorism financing, particularly the relations pertaining to the fight against money laundering and terrorism financing, the system of the bodies engaged in it, the rules for and terms of cooperation between these bodies, issues related to the supervision and application of responsibility measures in the field of combating money laundering and terrorism financing.

Reporting entities should have in place internal regulatory acts (rules, regulations, procedures, instructions, etc.) aimed at the prevention of money laundering and terrorism financing.

Reporting entities are obligated to have an Internal Monitoring Unit or a staff member engaged in combating money laundering and terrorism financing, or to delegate this function to a specialized entity.

Supervisors worldwide place special emphasis on the banks to have adequate control mechanisms and to know their customers. Proper identification of new customers, as well as measures taken for recognizing and preventing suspicious transactions and business relationships with customers are of key importance. This enables supporting the good reputation of the bank, restricting operational, legal, as well as concentration risk exposure while minimizing the probability for the banks to become an instrument or victim of financial crime.

Supervisors believe that the procedure for knowing the customer should become a constituent part of risk management and internal control systems of banks.

6.9.2. Objectives of Examining the Fight against Money Laundering and Terrorism Financing

1. Find out whether the policies, procedures, and internal control rules for combating money laundering and terrorism financing are sufficient for managing the relevant risks.
2. Find out whether the bank's staff observes the established principles.
3. Assess the scope and quality of activities of the Internal Audit.
4. Find out whether the Board and the executive management of the bank are aware of the tasks of procedures for combating money laundering and terrorism financing.
5. Find out whether the current laws and other legal statutes have been adhered to in the course of combating money laundering and terrorism financing.

6. In case of ascertaining inadequacy or absence of the bank's policies, procedures, and/ or internal control rules for the prevention of money laundering and terrorism financing, as well as uncovering violations of the laws and other legal statutes, make out recommendations for rectifying the deficiencies and eliminating the violations.

6.9.3. Procedure for Examining the Fight against Money Laundering and Terrorism Financing

1. Fill out the first column of the internal control examination checklist titled “Internal Regulatory Document”.
2. Examine compliance of the bank’s practices with the policies, procedures, and internal control rules adopted by the bank for the prevention of money laundering and terrorism financing.
3. Fill out the second column of the internal control examination checklist titled “Current Practice”.
4. Find out the measures taken for dealing with the violations and deficiencies (if any) uncovered by the previous inspection.
5. Request from the bank and examine the list of violations uncovered after the previous inspection (related to combating money laundering and terrorism financing) by the internal/ external audit, and find out the measures taken for eliminating such violations.
6. If necessary, review the scope and depth of the inspection based on the rating given to the internal control of the bank, on the analyses carried out by the Internal Monitoring Unit, and on the findings of the internal/ external audit.
7. Obtain and examine the description of the procedures for combating money laundering and terrorism financing, the patterns for arranging such procedures, including responsibilities of the staff, informational flows, confidentiality of information, dissemination of information to the Authorized Body, and control over the system.
8. Examine compliance of the bank’s policy for customer acceptance (opening accounts, executing transactions proposed by customers), customer identification (“Know Your Customer”), scrutiny of high-risk transactions and/ or business relationships, and risk management with the standards practiced internationally and/ or adopted by the Authorized Body.
9. Discuss with the staff of the CBA Financial Monitoring Center the deficiencies identified due to the examination, the examiner’s concerns about the bank’s practice in combating money laundering and terrorism financing.
10. Get acquainted with the staff of the bank’s customer service for getting an idea about their professionalism and awareness.
11. Examine how the bank carries out monitoring of its customers, their transactions and business relationships in order to detect extraordinary and suspicious receipts and withdrawals.
12. Discuss with the relevant manager of the bank and present to the inspection team leader analysis and conclusions on the following issues:
 - Exceptions stipulated by the internal control rules, uncovered shortcomings and deficiencies, as well as inconsistencies with the bank's policies and procedures;

- Deficiencies uncovered by the Internal Audit, which have not been rectified;
- Violations of laws and other legal statutes;
- Awareness of the responsible manager in the principles established by international organizations involved in combating money laundering and terrorism financing;
- Recommended corrective measures in case of detected deficiencies in the policies, procedures, or internal rules for combating money laundering and terrorism financing.

6.9.4. Internal Control Examination Checklist

Examine the bank's internal policy, practice, and procedures for combating money laundering and terrorism financing. The internal policy should be articulated in uniform documents and comprise interpretations, charts, and other supporting information.

Authorized/ Responsible Persons

1. Is there an Internal Monitoring Unit or a staff member in the bank engaged in combating money laundering and terrorism financing, or has this function been delegated to a specialized entity (hereinafter referred to as the Internal Monitoring Unit)? In banks, the function of internal monitoring can not be assigned to a staff member of the customer service.
2. Does the staff of the Internal Monitoring Unit have an appropriate qualification obtained in the manner and in compliance with the professional competence criteria established by the Authorized Body?
3. Does the bank have operational procedures for the Internal Monitoring Unit?
4. Does the Internal Monitoring Unit have direct access to all documents pertaining to the accounts and transactions of the customers (including credit files, working documents, contracts etc); is the Internal Monitoring Unit empowered to require clarifications from any staff member of other subdivisions on transactions and business relationships, as well as on customers, their authorized persons, and beneficial owners?
5. Does the Internal Monitoring Unit develop internal regulatory acts on combating money laundering and terrorism financing; carry out monitoring of effectiveness of their implementation; make recommendations on enhancing their effectiveness?
6. Does the Internal Monitoring Unit provide for the submission of reports and other information to the Authorized Body on behalf of the bank, as prescribed by the Law on Combating Money Laundering and Terrorism Financing?
7. Does the Internal Monitoring Unit review the compliance of the bank's transactions (business relationships), as well as of activities of its structural and territorial divisions and staff members with the Law on Combating Money Laundering and Terrorism Financing, with other normative legal statutes adopted on basis thereof, and with the internal regulatory acts, in the manner and at the periodicity established by the bank's internal regulatory acts, but no less than once in every six months?
8. Does the Internal Monitoring Unit report to the Board of the bank on the findings of the review and other issues raised by the Authorized Body?
9. Is the Internal Monitoring Unit independent in performing its functions, and does it have a status of senior management of the bank?

10. Does the Internal Monitoring Unit make the decision on suspending or rejecting a transaction or a business relationship, as well as on freezing terrorism-related funds?
11. Do the bank's internal regulatory acts establish the criteria and procedures for the Internal Monitoring Unit to notify the Board on the suspension or rejection of transactions or business relationships?
12. Is the Internal Monitoring Unit entitled to directly report – in the manner established by internal regulatory acts of the bank – to the bank's Board on the problems occurred in relation of preventing money laundering and terrorism financing?
13. Does the staff of the Internal Monitoring Unit carry out appropriate and efficient analyses to recognize suspicious transactions and business relationships?
14. Does the Internal Monitoring Unit oversee the ongoing monitoring of business relationships and periodically review the process of refining and updating available data; provide for the categorization of the bank's customers based on the risk profile; carry out ongoing monitoring of high-risk business relationships?
15. Does the Internal Monitoring Unit carry out monitoring of recordkeeping and data maintenance?
16. Do the regular reports of the Internal Monitoring Unit to the bank's Board comprise:
 - Information on the number of over-threshold and suspicious transactions and business relationships; a snapshot of suspicious transactions (business relationships);
 - Information on the number and comprehensive description of the transactions and business relationships, on which analyses have been carried out, though they have not been reported as suspicious transactions or business relationships;
 - Information on the number and a snapshot of suspended or rejected transactions and business relationships; the total amount of suspended transactions;
 - The total amount of frozen funds.
17. Does the bank at least once a year conduct internal audit to check appropriate performance of the duties stipulated by the Law on Combating Money Laundering and Terrorism Financing, by other legal statutes, and by the internal regulatory acts of the bank?
18. Does the Internal Audit regularly report to the Board and the executive management body on its findings and disclosures, including its conclusions on the relevance and efficiency of the AML/CFT staff training and professional development?
19. Does the bank commission external audit to check implementation and effectiveness of the legislation on combating money laundering and terrorism financing, in the manner established by the Authorized Body, upon the request of the Authorized Body or by their own initiative?

Internal Control System

20. Does the bank have internal procedures for collecting, recording, and maintaining data on its customers, as well as on suspicious transactions (business relationships)?
21. Do the bank's internal regulatory acts on recognizing suspicious transactions and business relationships and reporting to the Authorized Body provide for:

- The procedures for communicating to the Internal Monitoring Unit the preliminary information (assumptions) on suspicious transactions or business relationships;
 - The rules and deadlines for the Internal Monitoring Unit to process, verify, and put forward possible conclusions on suspicious transactions or business relationships;
 - The possible actions and analyses for recognizing suspicious transactions or business relationships, including the access to national and international databases, the requests, the criteria for assessing their results, and the rules for summarizing such results.
22. Does the bank have a list of the documents and other information required for regular and enhanced due diligence?
 23. Does the bank have internal procedures for suspending (rejecting) suspicious transactions (business relationships); freezing funds of terrorism-related persons?
 24. Does the bank have internal regulatory acts on current risks and typologies of money laundering and terrorism financing?
 25. Does the bank have internal procedures for reporting to the Authorized Body?
 26. Do the bank's internal regulatory acts define the cases (besides the ones defined by the Authorized Body) when 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, or that the funds or other assets are linked to or intended for use by terrorist organizations or individual terrorists for the purpose of terrorism (suspicious transactions or business relationships)?
 27. Do the bank's internal regulatory acts define criteria evidencing the high likelihood of money laundering and terrorism financing (high-risk criteria, i.e. persons, situations, or subjects matching the definitions provided by the Regulation on the Minimal Requirements Stipulated for Financial Institutions in the Area of Combating Money Laundering and Terrorist Financing, as approved by the Decision No 269-N of September 9, 2008 of the Board of the Republic of Armenia Central Bank)?
 28. Do the bank's internal regulatory acts provide for and apply relevant measures for counteracting money laundering or terrorism financing risks associated with new or developing technologies?
 29. Do the bank's internal regulatory acts provide for preventive mechanisms to address all risks associated with non face-to-face transactions or business relationships, when establishing business relationships or conducting ongoing due diligence of their customers?
 30. Is there an appropriate system of control and monitoring so as to timely recognize suspicious transactions, and to file prompt and accurate reports with the Authorized Body?
 31. Do the bank's internal regulatory acts establish the procedure for information exchange between relevant staff of the bank in case of detecting suspicious transactions?
 32. Does the bank ensure confidentiality of information on suspicious transactions?

Customer Identification System

33. Does the bank have internal regulatory acts establishing the procedure for the identification of customers and third parties/ authorized persons acting on their behalf, the required documents (information), including information on new customers, as well as on the customers offering

the bank to carry out transactions or to enter into business relationships without their physical presence? Does the bank receive the identification documents (information) and check their veracity before establishing a business relationship or concluding an occasional transaction, or in the course of establishing a business relationship or concluding an occasional transaction or thereafter within a reasonable timeframe, 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?

34. Do the bank's internal regulatory acts provide for necessary measures to find out the existence of beneficial owners and, if available, to identify and verify their identity?
35. Are there defined criteria for the risk-based categorization of customers?
36. If the customer or the other party to the transaction is a foreign legal person or a foreign natural person or an entity without legal personality under foreign law, does the bank also identify and document the center of vital interests and the sources of income of these persons?
37. Does the bank have internal procedures establishing procedures for termination of business relationships in case of suspicious transactions associated with intentional distortion of the data submitted by customers?
38. Does the bank have risk management procedures laid down in its internal regulatory acts so as to determine whether the customer is a politically exposed person or a member of his family or a person affiliated to him, or whether there are other criteria of high risk?
39. Do the bank's internal regulatory acts provide for measures to establish the source of income (wealth) and the origin of funds of the customers or beneficial owners identified as politically exposed persons?
40. Do the bank's internal regulatory acts require that, in the presence of high risk criteria, enhanced customer due diligence is performed?
41. While performing enhanced due diligence, does the bank:
 - Carry out more comprehensive and in-depth check of the veracity of the documents (information) required for establishing business relationships with the customer;
 - Require information on the source of the customer's assets and other funds;
 - Examine the information on the customer, the business relationship, and the transaction through various databases;
 - Make requests to other reporting entities or to other bodies, including foreign counterparts, to check the information on the customer, on his business relationships and occasional transactions.
42. Is the approval of the bank's senior management obtained before establishing or for continuing business relationships with customers identified as politically exposed persons; as well as in cases, when the customer or the beneficial owner is subsequently found to be or becomes a politically exposed person?
43. Does the bank conduct additional scrutiny of all complex and unusually large transactions (business relationships), as well as of the ones involving unusual patterns with no apparent economic or other legitimate purpose?

44. Do the bank's internal regulatory acts establish the rules for opening and maintaining correspondent accounts of foreign banks, as well as the peculiarities of opening and maintaining their correspondent accounts with foreign banks so as to make sure that they have not established correspondent relationships with shell banks or with banks allowing shell banks to use their accounts? Do these acts define the information considered to be sufficient for fully understanding the nature of respondent bank's business and for determining the business reputation of the respondent bank and the quality of its supervision, including whether it has been subject to a money laundering or terrorism financing criminal investigation or any other proceeding?
45. Is the approval of the bank's senior management obtained before establishing new correspondent relationships?
46. Does the bank have procedures for documenting the respective functions of each correspondent bank?
47. Does the bank have procedures for ascertaining that, with respect to payable-through accounts, the respondent bank has verified the identify of the customers having access to its accounts and continuously conducts their ongoing monitoring, and that upon request it would be able to provide relevant customer identification data to the correspondent bank?
48. Does the bank conduct ongoing customer due diligence throughout the course of business relationships?
49. Does the bank have procedures for conducting monitoring of the transactions with the customer in the course of customer due diligence so as to ascertain veracity of the information on the customer, his business and risk profile and, where necessary, of the sources of his income?
50. Does the bank update the data obtained due to customer identification, at a periodicity determined by its own?
51. Does the bank identify and verify the identity of the originators when carrying out wire transfers, regardless of the fact of opening an account?
52. For the purpose of customer identification and verification of identity, does the bank obtain and maintain the following information about the originator of the transfer:
 - Forename and surname;
 - Account number (in its absence, the unique reference number accompanying the transfer);
 - Details of the identification document.
53. Is that information, including the account number of the originator (in its absence, the unique reference number accompanying the transfer) included in the payment order accompanying the transfer?
54. Do the bank's internal regulatory acts provide for conducting enhanced due diligence when establishing business relationships or carrying out transactions with persons domiciled in foreign countries or territories, which are in non-compliance or inadequate compliance with the international requirements on combating money laundering and terrorism financing?
55. Do the branches and representative offices of the bank domiciled in foreign countries or territories (if any) apply the requirements of the Law on Combating Money Laundering and

Terrorism Financing and of other legal statutes adopted on the basis thereof, if these establish norms stricter than those established by the laws and other legal statutes applicable in the country of domicile of such branches or representative offices?

56. Does the bank carry out regular analysis of the dynamics and risk profile of customer transactions; particularly to ensure that:
- The existing interrelation between the transactions, the possible schemes of such interrelations, as well as the objectives of the transactions are disclosed;
 - The substance of the transactions corresponds to the type of activities performed by the customer;
 - Possible information on the customer's sources of income is collected;
 - The sources of funds, their movement and volumes of transaction are compared;
 - The possible money laundering and terrorism financing risks pertinent to the transaction or business relationships are assessed by means of comparing them with the grounds and criteria of suspicious transactions and business relationships;
 - It is checked whether there are business relationships and (or) occasional transactions, with which the customer aims to avoid being reported by the bank to the Authorized Body;
 - The types, periodicity, and chronology of the transaction within a certain period of time are checked;
 - Data on transaction parties, recipients, beneficial owners, as well as on authorized persons is recorded and compared so as to identify interrelations between customers; and
 - Other measures stipulated by the bank's internal regulatory acts are performed.

Recordkeeping

57. Is recordkeeping in the bank arranged through classified databases, so as to be able to restore the data of the staff member having performed identification or other actions subject to recordkeeping?
58. Does the bank ensure the security and confidentiality of recorded and maintained information, and prevent its unauthorized use and possession?
59. Does the bank record and maintain:
- Customer identification data;
 - Data on the main conditions of the transaction (business relationships);
 - Data on any analysis and other measures taken for detecting suspicious transactions or business relationships;
 - Suspicious transaction reports, as well as the underlying information and the minutes of deliberations concerning the submission of such reports; and
 - Data and assumptions on transactions or business relationships, with regard to which no reports on suspicious transactions or business relationships have been filed with the Authorized Body.
60. Do the internal regulatory acts establish that the bank should maintain customer identification data, including account files and transaction details, business correspondence, as well as data on transactions (business relationships) subject to additional scrutiny – for at least 5 years

following conduction of the transaction or completion of the business relationship or, in cases prescribed by law, for a longer period?

61. Do the internal regulatory acts establish that the bank should maintain data on the main conditions of the transaction (business relationship), so as to permit full reconstruction of individual transactions (business relationships) – for at least 5 years following conduction of the transaction or completion of the business relationship or, in cases prescribed by law, for a longer period?
62. Are the programs for the training of the bank's staff, as well as other information relevant to training separately recorded and maintained for at least 5 years?
63. Are the names and signatures of the bank's staff having participated in training programs recorded and maintained for at least 5 years?

Staff

64. Is the staff of the customer service aware of the criteria of suspicious transactions or business relationships?
65. Is the bank's staff aware of the transactions or business relationships subject to reporting to the Authorized Body?
66. Is the bank's staff aware of the prohibition to inform the person, on whom a report or other information has been submitted to the Authorized Body, as well as other persons, about the fact of having submitted such report or information?
67. Is the bank's staff involved in the prevention of money laundering and terrorism financing regularly trained on the matter of their duties and responsibilities? In case of hiring new personnel, does the bank organize trainings on combating money laundering and terrorism financing within the first three months of their employment?
68. Is there a program for the professional development of the staff specifying the periodicity, themes, positions, and other pertinent minimal requirements with regard to training?
69. Is there designated staff in the bank responsible for the organization and implementation of training programs?
70. Is the relevant staff of the bank, particularly the Board members, the AML/CFT authorized/responsible staff, the staff doing customer identification familiar with the bank's internal regulatory acts on the prevention of ML/ FT and with the requirements of the national legislation in respect of combating ML/ FT?
71. Does the Board of the bank:
 - Set forth the bank's policy in combating ML/FT;
 - Adopt the annual programs of the Internal Monitoring Unit and the Internal Audit in the field of ML/FT prevention, approve their performance reports; as well as oversee the implementation of such programs;
 - In case of need, initiate studies by the Internal Monitoring Unit in the field of preventing ML/FT; approve the measures aimed at the elimination of shortcomings identified due to the audit or other controls; and oversee their implementation;
 - Approve and amend the internal regulatory acts on ML/FT prevention;

- Receive and consider the reports of the Internal Monitoring Unit and (or) the Internal Audit on the performance in the implementation of internal regulatory acts, at the periodicity established by it;
 - Oversee the efficiency of the internal system for ML/FT prevention.
72. Does the executive management body of the bank:
- Ensure comprehensive and effective application of internal regulatory acts;
 - Ensure implementation of the policy and procedures for combating ML/FT as defined by the Board of the bank;
 - Appoint and dismiss the head and the staff members of the Internal Monitoring Unit upon the approval of the Board;
 - Ascertain that the staff of the bank is fluent in internal regulatory acts for combating ML/FT, as well as in the code of ethics; ensure arrangement of the training and professional development of the staff in the field of combating ML/TF;
 - Ensure conduction of customer due diligence, including simplified or enhanced due diligence, ongoing monitoring, as well as obtaining, recording, and updating of information;
 - Provide material and technical resources for the Internal Monitoring Unit;
 - Implement measures aimed at the elimination of the shortcomings identified due to the examinations of the Internal Monitoring Unit, audit or other controls.
73. Do the bank's internal regulatory acts establish the staff responsibility in case of violating the provisions of the internal regulatory acts on prevention of ML/ FT?

ANNEX 28 – DECISION OF THE CHAIRMAN OF THE REPUBLIC OF ARMENIA CENTRAL BANK No 1/1178L of NOVEMBER 28, 2008 (ON ON-SITE INSPECTIONS IN CREDIT ORGANIZATIONS)

Based on Article 18 of the Republic of Armenia Law on the Central Bank of the Republic of Armenia, I:

DECIDE

1. When conducting on-site inspections in credit organizations, to be guided by the Manual on On-Site Inspections in Banks approved by the Decision of the Chairman of the Central Bank No 1/637L of July 27, 2006⁴⁰, taking into consideration peculiarities of credit organizations; particularly, for the purposes of inspection:

1.1 Disregard the chapters “Deposits and Bank Accounts”, “Payment System Risks”, and “Electronic Transfer of Funds”;

1.2. Disregard the areas pertaining to the calculation of the composite CAMELS rating, as well as all transactions and procedures, which are characteristic for banks and are not applicable to credit organizations.

2. This Decision shall enter into force on the next day of its signing.

Vache Gabrielyan

Vice Chairman

⁴⁰ As amended by the Decision of the Chairman of the Republic of Armenia Central Bank No 1-1315L of October 19, 2009.

ANNEX 29 – EXTRACT FROM THE DECISION OF THE CHAIRMAN OF THE REPUBLIC OF ARMENIA CENTRAL BANK No 1-1454A of NOVEMBER 25, 2009 (ON ON-SITE INSPECTIONS IN INSURANCE COMPANIES)

8.2. Combating Money Laundering and Terrorism Financing

8.2.1. Introduction

In the international practice, insurance industry is considered to be among those exposed to the risk of money laundering and terrorist financing (hereinafter referred to as ML/TF) due to its volumes, wide access to and diversity of insurance services, international coverage of the insurance business, as well as broad involvement of insurance intermediaries. Disclosure of money laundering and terrorist financing, in turn, is rather a sophisticated process conditioned by the hidden and chain-type nature of this crime and, of course, by its international occurrence.

Supervisors worldwide place special emphasis on the insurance companies to have adequate control mechanisms and to know their customers. Proper identification of new customers, as well as measures taken for recognizing and preventing suspicious transactions and business relationships with customers are of key importance. This enables supporting the good reputation of the insurance company, restricting operational, legal, as well as concentration risk exposure while minimizing the probability for the insurance companies to become an instrument or victim of financial crime.

In the capacity of the Authorized Body for combating money laundering and terrorism financing, the Central Bank places special emphasis on the insurance companies to take measures in the manner established by law and other legal statutes for recognizing and preventing suspicious transactions (business relationships) of their customers or third parties.

Due to the examination of this field, supervisors should ascertain that the policy, procedures, and internal control rules are sufficient for disclosing and preventing money laundering and terrorism financing. For that purpose, supervisors should examine the internal procedures in the insurance company for disclosing potential ML/TF attempts and cases, the systems for obtaining and maintaining customer identification and other data, the awareness and professionalism of the company staff, including of those involved in customer service.

8.2.2. Objectives of Examining the Fight against Money Laundering and Terrorism Financing

7. Find out whether the insurance company has an ML/TF prevention policy, which:
 - a. Is sufficient for managing the relevant risks of the company;
 - b. Complies with the requirements of laws and other legal statutes (appropriate policy).
8. Find out whether the insurance company operates in compliance with the established policy (appropriate implementation).
9. Examine whether the insurance company obtains and maintains information required for combating ML/TF; whether there is an appropriate practice of reporting to the Authorized Body over-threshold transactions, as well as suspicious transactions and business relationships (appropriate recordkeeping).

10. Ascertain that the insurance company is not involved in any ML/TF process (assessment of risk).
11. Check whether violations of current laws and other legal statutes have occurred while establishing and implementing the policy for combating ML/TF (legal compliance).

8.2.3. Procedure for Examining the Fight against Money Laundering and Terrorism Financing

Appropriate Policy

1. Find out whether the insurance company has an ML/TF prevention policy.
2. In case of positive answer, examine policy documents and assess their efficiency.
3. Find out whether the insurance company's policy for ML/TF prevention at least defines:
 - 1) The procedures for conducting customer due diligence and maintaining information;
 - 2) The list of the documents and other information required for regular and enhanced due diligence;
 - 3) The manner and rules for conducting internal audit to check observance of procedures and requirements established by internal regulatory acts;
 - 4) The internal procedures for the activities of the Internal Monitoring Unit;
 - 5) The procedures for obtaining, recording, and maintaining information on suspicious and other transactions (business relationships);
 - 6) The internal procedures for suspending (rejecting) suspicious transactions (business relationships); freezing funds of terrorism-related persons;
 - 7) The requirements with respect to the hiring, training, and professional development of the staff of the Internal Monitoring Unit or other staff members performing relevant functions as defined under the law, in areas such as the legislation on combating money laundering and terrorism financing, other legal statutes (particularly those on customer due diligence and suspicious transaction reporting obligations), as well as the current risks and typologies of money laundering and terrorism financing;
 - 8) The criteria of suspicious transactions and business relationships;
 - 9) The internal procedures for reporting to the Authorized Body.
4. Discuss with the company management the changes entered/ intended to be entered in the ML/TF prevention policy and internal procedures; assess relevance of such changes.
5. Examine whether the company's ML/TF prevention policy takes into consideration the nature and peculiarities of activities of the company or, rather, it is a reiteration of the requirements of applicable laws and normative legal statutes in the field of combating ML/TF.

Appropriate Implementation

6. Examine whether the management and the staff of the insurance company act in compliance with the established policy.

Appropriate Recordkeeping

7. Examine whether the insurance company appropriately records and maintains the following information:
 - 1) Customer identification data;
 - 2) Data on the main conditions of the transaction (business relationships);
 - 3) Data on any analysis and other measures taken for detecting suspicious transactions or business relationships;
 - 4) Suspicious transaction reports, as well as the underlying information and the minutes of deliberations concerning the submission of such reports; and
 - 5) Data and assumptions on transactions or business relationships, with regard to which no reports on suspicious transactions or business relationships have been filed with the Authorized Body.
8. Check whether recordkeeping in the insurance company is arranged through classified databases, so as to enable establishing the staff member having performed identification or other actions subject to recordkeeping.
9. Examine the log files of the Internal Monitoring Unit on suspicious transactions (business relationships); particularly:
 - 1) Compare the reports on suspicious transactions or business relationships submitted to the Internal Monitoring Unit by the customer service staff of the insurance company with those filed with the Authorized Body;
 - 2) Ascertain that, in cases when the transactions or business relationships recognized suspicious by the relevant staff have not been reported to the Authorized Body, the insurance company has reasonable justification for that.
10. Check whether all over-threshold transactions have been duly reported to the Authorized Body.
11. Check whether the insurance company ensures the security and confidentiality of recorded and maintained information, and prevent its unauthorized use and possession.
12. Examine whether the insurance company maintains customer identification data, as well as data on transactions (business relationships) subject to additional scrutiny – for at least 5 years following conduction of the transaction or completion of the business relationship or, in cases prescribed by law, for a longer period.
13. Examine whether the insurance company maintains data on the main conditions of the transaction (business relationship), so as to permit full reconstruction of individual transactions (business relationships) – for at least 5 years following conduction of the transaction or completion of the business relationship or, in cases prescribed by law, for a longer period.
14. Find out whether the insurance company updates customer data, at a periodicity determined by its internal regulatory acts.
15. Find out whether the programs for the training of the insurance company’s staff, as well as other information relevant to training is separately recorded and maintained for at least 5 years.
16. Find out whether the names and signatures of the insurance company’s staff having participated in training programs are recorded and maintained for at least 5 years.

Assessment of Risk

17. Examine the description of the procedures for combating money laundering and terrorism financing, the patterns for arranging such procedures, including responsibilities of the staff, informational flows, confidentiality of information, dissemination of information to the Authorized Body, and control over the system.
18. For the prevention of ML/TF, special attention should be paid to the following types of transactions (activities):
 - 1) Early terminated insurance contracts, particularly:
 - a. Contracts with the same insurer, providing for small insurance contributions and terminated on the same day before the end of the contract;
 - b. Contracts for which the refunded insurance contributions have been transferred to an account different from the one used for making such contributions;
 - c. Regular conclusions and early terminations of insurance contracts;
 - 2) Insurance contracts providing for high commission fees;
 - 3) Over-estimated or fraudulent insurance payments;
 - 4) Any other transaction (activity) which supervisors consider to be suspicious and (or) unusual.
19. Examine compliance of the insurance company's policy for customer service, customer identification ("Know Your Customer"), scrutiny of high-risk transactions and/ or business relationships, and risk management with the standards practiced internationally and/ or adopted by the Authorized Body.
20. Get acquainted with the staff of the insurance company's customer service for getting an idea about their professionalism and awareness in the applicable legislation on combating ML/TF and relevant internal regulatory acts.
21. Examine how the insurance company carries out monitoring of its customers, their transactions and business relationships in order to detect extraordinary and suspicious receipts and withdrawals.
22. Discuss with the staff of the CBA Financial Monitoring Center the deficiencies identified due to the examination, the examiner's concerns about the insurance company's practice in combating money laundering and terrorism financing.

Legal Compliance

23. Ascertain that the requirements of current laws and other legal statutes have not been violated in the course of combating ML/TF.

8.2.4. Procedure for Examining Internal Control

Appropriate Policy

1. Find out whether the insurance company has internal procedures for defining an ML/TF prevention policy.

2. Find out whether the Internal Monitoring Unit regularly monitors effectiveness of implementation of the ML/TF prevention policy, makes recommendations on enhancing its effectiveness.
3. Find out whether the opinion of other stakeholders is taken into consideration while defining the ML/TF prevention policy.
4. Find out whether the insurance company has clearly articulated internal procedures for the company's staff members and other stakeholders to make recommendations on necessary revisions of the ML/TF prevention policy.
5. Find out whether the ML/TF prevention policy, before being approved by the Board of the insurance company, is checked for compliance with the requirements of current legislation.
6. Check whether the ML/TF prevention policy and the changes therein are approved by the Board of the insurance company.
7. Find out whether the ML/TF prevention policy is regularly (at least once a year) revised to take into consideration the changes in the activities of the insurance company, the principles set forth by involved international organizations, and the practical examples of ML/TF typologies.

Appropriate Application

8. Find out whether there are internal procedures to control implementation of the ML/TF prevention policy.
9. Find out whether the insurance company at least once a year conducts internal audit to check appropriate performance of the duties stipulated by the Law on Combating Money Laundering and Terrorism Financing, by other legal statutes, and by the internal regulatory acts of the insurance company.
10. Find out whether the Internal Audit regularly reports to the Board and the executive management body on its findings and disclosures, including its conclusions on the relevance and efficiency of the AML/CFT staff training and professional development.
11. Find out whether the insurance company commissions external audit to check implementation and effectiveness of the legislation on combating money laundering and terrorism financing, in the manner established by the Authorized Body, upon the request of the Authorized Body or by their own initiative.
12. Find out whether there are mechanisms for imposing disciplinary sanctions on the company staff in case of violation of the ML/TF prevention policy.

Appropriate Recordkeeping

13. Find out whether the insurance company has internal procedures for collecting, recording, and maintaining data on its customers, as well as on suspicious transactions (business relationships).
14. Find out whether the insurance company's internal regulatory acts on recognizing suspicious transactions and business relationships and reporting to the Authorized Body provide for:
 - The procedures for communicating to the Internal Monitoring Unit the preliminary information (assumptions) on suspicious transactions or business relationships;

- The rules and deadlines for the Internal Monitoring Unit to process, verify, and put forward possible conclusions on suspicious transactions or business relationships;
 - The possible actions and analyses for recognizing suspicious transactions or business relationships, including the access to national and international databases, the requests, the criteria for assessing their results, and the rules for summarizing such results.
15. Find out whether the Internal Monitoring Unit monitors recordkeeping and maintenance of information.
 16. Find out whether the insurance company has internal procedures for reporting to the Authorized Body.

Assessment of Risk

17. Find out whether there is an Internal Monitoring Unit or a staff member in the insurance company engaged in combating money laundering and terrorism financing, or has this function been delegated to a specialized entity (hereinafter referred to as the Internal Monitoring Unit). In insurance companies, the function of internal monitoring can not be assigned to a staff member of the customer service.
18. Find out whether the Internal Monitoring Unit is independent in performing its functions and has a status of senior management of the insurance company.
19. Find out whether the insurance company has operational procedures for the Internal Monitoring Unit.
20. Find out whether the Internal Monitoring Unit has direct access to all documents pertaining to concluded insurance contracts and performed transactions, whether it is empowered to require clarifications from any staff member of other subdivisions on transactions and business relationships, as well as on customers, their authorized persons, and beneficial owners.
21. Find out whether the Internal Monitoring Unit reviews the compliance of the insurance company's transactions (business relationships), as well as of activities of its structural and territorial divisions and staff members with the Law on Combating Money Laundering and Terrorism Financing, with other normative legal statutes adopted on basis thereof, and with the internal regulatory acts, in the manner and at the periodicity established by the insurance company's internal regulatory acts, but no less than once in every six months.
22. Find out whether the Internal Monitoring Unit reports to the Board of the insurance company on the findings of the review and other issues raised by the Authorized Body
23. Find out whether the Internal Monitoring Unit makes the decision on suspending or rejecting a transaction or a business relationship, as well as on freezing terrorism-related funds.
24. Find out whether the insurance company's internal regulatory acts establish the criteria and procedures for the Internal Monitoring Unit to notify the Board on the suspension or rejection of transactions or business relationships.
25. Find out whether the staff of the Internal Monitoring Unit carries out appropriate and efficient analyses to recognize suspicious transactions and business relationships.
26. Find out whether the Internal Monitoring Unit oversees the ongoing monitoring of business relationships and periodically reviews the process of refining and updating available data;

- provides for the categorization of the insurance company's customers based on the risk profile; carries out ongoing monitoring of high-risk business relationships.
27. Find out whether the insurance company has a list of the documents and other information required for regular and enhanced due diligence.
 28. Find out whether the insurance company has internal procedures for suspending (rejecting) suspicious transactions (business relationships); freezing funds of terrorism-related persons.
 29. Find out whether the insurance company's internal regulatory acts define the cases (besides the ones defined by the Authorized Body) when 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, or that the funds or other assets are linked to or intended for use by terrorist organizations or individual terrorists for the purpose of terrorism (suspicious transactions or business relationships).
 30. Find out whether the insurance company's internal regulatory acts define criteria evidencing the high likelihood of money laundering and terrorism financing (high-risk criteria, i.e. persons, situations, or subjects matching the definitions provided by the Regulation on the Minimal Requirements Stipulated for Financial Institutions in the Area of Combating Money Laundering and Terrorist Financing, as approved by the Decision No 269-N of September 9, 2008 of the Board of the Republic of Armenia Central Bank).
 31. Find out whether the insurance company's internal regulatory acts provide for and apply relevant measures for counteracting money laundering or terrorism financing risks associated with new or developing technologies.
 32. Find out whether the insurance company's internal regulatory acts provide for preventive mechanisms to address all risks associated with non face-to-face transactions or business relationships, when establishing business relationships or conducting ongoing due diligence of their customers.
 33. Find out whether there is an appropriate system of control and monitoring so as to timely recognize suspicious transactions, and to file prompt and accurate reports with the Authorized Body.
 34. Find out whether the insurance company's internal regulatory acts provide for the procedures for the relevant staff to communicate to the Internal Monitoring Unit the preliminary information (assumptions) on suspicious transactions or business relationships.
 35. Find out whether the insurance company ensures confidentiality of information on suspicious transactions.
 36. Find out whether the insurance company's staff involved in the prevention of money laundering and terrorism financing is regularly trained on the matter of their duties and responsibilities; whether, in case of hiring new personnel, the insurance company organizes trainings on combating money laundering and terrorism financing within the first three months of their employment.
 37. Find out whether there a program for the professional development of the staff specifying the periodicity, themes, positions, and other pertinent minimal requirements with regard to training.

38. Find out whether there is designated staff in the insurance company responsible for the organization and implementation of training programs.
39. Find out whether there are defined criteria for categorizing the customers based on the risk profile, and special rules are applied to high-risk customers.
40. Find out whether the insurance company has risk management procedures laid down in its internal regulatory acts so as to determine whether the customer is a politically exposed person or a member of his family or a person affiliated to him, or whether there are other criteria of high risk.
41. Find out whether the insurance company's internal regulatory acts provide for measures to establish the source of income (wealth) and the origin of funds of the customers or beneficial owners identified as politically exposed persons.
42. Find out whether the insurance company's internal regulatory acts require that, in the presence of high risk criteria, enhanced customer due diligence is performed.
43. While performing enhanced due diligence, does the insurance company:
 - 1) Carry out more comprehensive and in-depth check of the veracity of the documents (information) required for establishing business relationships with the customer;
 - 2) Require information on the source of the customer's assets and other funds;
 - 3) Examine the information on the customer, the business relationship, and the transaction through various databases;
 - 4) Make requests to other reporting entities or to other bodies, including foreign counterparts, to check the information on the customer, on his business relationships and occasional transactions;
 - 5) Take other measures to get a comprehensive and full understanding of the customer, the transactions performed by him and the business relationships established with him.
44. Find out whether the insurance company conducts additional scrutiny of all complex and unusually large transactions (business relationships), as well as of the ones involving unusual patterns with no apparent economic or other legitimate purpose.
45. Find out whether the insurance company carries out regular analysis of the dynamics and risk profile of customer transactions; particularly to ensure that:
 - 1) The existing interrelation between the transactions, the possible schemes of such interrelations, as well as the objectives of the transactions are disclosed;
 - 2) The substance of the transactions corresponds to the type of activities performed by the customer;
 - 3) Possible information on the customer's sources of income is collected;
 - 4) The sources of funds, their movement and volumes of transaction are compared;
 - 5) The possible money laundering and terrorism financing risks pertinent to the transaction or business relationships are assessed by means of comparing them with the grounds and criteria of suspicious transactions and business relationships;
 - 6) It is checked whether there are business relationships and (or) occasional transactions, with which the customer aims to avoid being reported by the insurance company to the Authorized Body;

- 7) The types, periodicity, and chronology of the transaction within a certain period of time are checked;
- 8) Data on transaction parties, recipients, beneficial owners, as well as on authorized persons is recorded and compared so as to identify interrelations between customers; and
- 9) Other measures stipulated by the insurance company's internal regulatory acts are performed.

Legal Compliance

46. Find out whether the procedures ensure the insurance company's compliance with the requirements of the Law on Combating Money Laundering and Terrorism Financing and of other legal statutes.

ANNEX 30 - EXTRACT FROM THE DECISION OF THE CHAIRMAN OF THE REPUBLIC OF ARMENIA CENTRAL BANK No 1/139A of FEBRUARY 24, 2010 (ON ON-SITE INSPECTIONS IN INVESTMENT COMPANIES)

6.2. Combating Money Laundering and Terrorism Financing

6.2.1. Introduction

Disclosure of money laundering and terrorist financing is rather a sophisticated process conditioned by the hidden and chain-type nature of this crime and, of course, by its international occurrence.

Supervisors worldwide place special emphasis on the investment companies to have adequate control mechanisms and to know their customers. Proper identification of new customers, as well as measures taken for recognizing and preventing suspicious transactions and business relationships with customers are of key importance. This enables supporting the good reputation of the investment company, restricting operational, legal, as well as concentration risk exposure while minimizing the probability for the investment companies to become an instrument or victim of financial crime.

In the capacity of the Authorized Body for combating money laundering and terrorism financing, the Central Bank places special emphasis on the investment companies to take measures in the manner established by law and other legal statutes for recognizing and preventing suspicious transactions (business relationships) of their customers or third parties.

Due to the examination of this field, supervisors should ascertain that the policy, procedures, and internal control rules are sufficient for disclosing and preventing money laundering and terrorism financing. For that purpose, supervisors should examine the internal procedures in the investment company for disclosing potential ML/TF attempts and cases, the systems for obtaining and maintaining customer identification and other data, the awareness and professionalism of the company staff, including of those involved in customer service.

6.2.2. Objectives of Examining the Fight against Money Laundering and Terrorism Financing

12. Find out whether the investment company has a policy for combating ML/TF, which:
 - a. Is sufficient for managing the relevant risks of the company;
 - b. Complies with the requirements of laws and other legal statutes (appropriate policy).
13. Find out whether the investment company operates in compliance with the established policy (appropriate implementation).
14. Examine whether the investment company obtains and maintains information required for combating ML/TF; whether there is an appropriate practice of reporting to the Authorized Body over-threshold transactions, as well as suspicious transactions and business relationships (appropriate recordkeeping).
15. Ascertain that the investment company is not involved in any ML/TF process (assessment of risk).

16. Check whether violations of current laws and other legal statutes have occurred while establishing and implementing the policy for combating ML/TF (legal compliance).

6.2.3. Procedure for Examining the Fight against Money Laundering and Terrorism Financing

Appropriate Policy

24. Find out whether the investment company has a policy for combating ML/TF.
25. In case of positive answer, examine policy documents and assess their efficiency.
26. Find out whether the investment company's policy for combating ML/TF at least defines:
 - 1) The procedures for conducting customer due diligence and maintaining information;
 - 2) The list of the documents and other information required for regular and enhanced due diligence;
 - 3) The manner and rules for conducting internal audit to check observance of procedures and requirements established by internal regulatory acts;
 - 4) The internal procedures for the activities of the Internal Monitoring Unit;
 - 5) The procedures for obtaining, recording, and maintaining information on suspicious and other transactions (business relationships);
 - 6) The internal procedures for suspending (rejecting) suspicious transactions (business relationships); freezing funds of terrorism-related persons;
 - 7) The requirements with respect to the hiring, training, and professional development of the staff of the Internal Monitoring Unit or other staff members performing relevant functions as defined under the law, in areas such as the legislation on combating money laundering and terrorism financing, other legal statutes (particularly those on customer due diligence and suspicious transaction reporting obligations), as well as the current risks and typologies of money laundering and terrorism financing;
 - 8) The criteria of suspicious transactions and business relationships;
 - 9) The procedures for the Internal Monitoring Unit to notify the authorized governance body on the suspension or rejection of transactions or business relationships;
 - 10) The procedures for the relevant staff to communicate to the Internal Monitoring Unit the preliminary information (assumptions) on suspicious transactions or business relationships;
 - 11) The internal procedures for reporting to the Authorized Body;
 - 12) The cases (besides the ones defined by the Authorized Body) when 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, or that the funds or other assets are linked to or intended for use by terrorist organizations or individual terrorists for the purpose of terrorism (suspicious transactions or business relationships);
 - 13) The criteria evidencing the high likelihood of money laundering and terrorism financing (high-risk criteria, i.e. persons, situations, or subjects matching the definitions provided by the Regulation on the Minimal Requirements Stipulated for Financial Institutions in the Area of Combating Money Laundering and Terrorist Financing, as approved by the

Decision No 269-N of September 9, 2008 of the Board of the Republic of Armenia Central Bank);

- 14) The risk management procedures to determine whether the customer is a politically exposed person or a member of his family or a person affiliated to him, or whether there are other criteria of high risk.
 - 15) The measures for establishing the source of income (wealth) and the origin of funds of the customers or beneficial owners identified as politically exposed persons;
 - 16) The preventive mechanisms to address all risks associated with non face-to-face transactions or business relationships, when establishing business relationships or conducting ongoing due diligence of their customers.
27. Discuss with the company management the changes entered/ intended to be entered in the policy for combating ML/TF and internal procedures; assess relevance of such changes.
 28. Examine whether the company's policy for combating ML/TF takes into consideration the nature and peculiarities of activities of the company or, rather, it is a reiteration of the requirements of applicable laws and normative legal statutes in the field of combating ML/TF.

Appropriate Implementation

Examine whether the management and the staff of the investment company act in compliance with the established policy.

Appropriate Recordkeeping

1. Examine whether the investment company appropriately records and maintains the following information:
 - 1) Customer identification data;
 - 2) Data on the main conditions of the transaction (business relationships);
 - 3) Data on any analysis and other measures taken for detecting suspicious transactions or business relationships;
 - 4) Suspicious transaction reports, as well as the underlying information and the minutes of deliberations concerning the submission of such reports; and
 - 5) Data and assumptions on transactions or business relationships, with regard to which no reports on suspicious transactions or business relationships have been filed with the Authorized Body.
2. Check whether recordkeeping in the investment company is arranged through classified databases, so as to enable establishing the staff member having performed identification or other actions subject to recordkeeping.
3. Examine the log files of the Internal Monitoring Unit on suspicious transactions (business relationships); particularly:
 - 1) Compare the reports on suspicious transactions or business relationships submitted to the Internal Monitoring Unit by the customer service staff of the investment company with those filed with the Authorized Body;

- 2) Ascertain that, in cases when the transactions or business relationships recognized suspicious by the relevant staff have not been reported to the Authorized Body, the investment company has reasonable justification for that.
4. Check whether all over-threshold transactions have been duly reported to the Authorized Body.
5. Check whether the investment company ensures the security and confidentiality of recorded and maintained information, and prevent its unauthorized use and possession.
29. Examine whether the investment company maintains customer identification data, as well as data on transactions (business relationships) subject to additional scrutiny – for at least 5 years following conduction of the transaction or completion of the business relationship or, in cases prescribed by law, for a longer period.
30. Examine whether the investment company maintains data on the main conditions of the transaction (business relationship), so as to permit full reconstruction of individual transactions (business relationships) – for at least 5 years following conduction of the transaction or completion of the business relationship or, in cases prescribed by law, for a longer period.
31. Find out whether the investment company updates customer data, at a periodicity determined by its internal regulatory acts.
32. Find out whether the programs for the training of the investment company’s staff, as well as other information relevant to training is separately recorded and maintained for at least 5 years.
33. Find out whether the names and signatures of the investment company’s staff having participated in training programs are recorded and maintained for at least 5 years.

Assessment of Risk

1. Examine the description of the procedures for combating money laundering and terrorism financing, the patterns for arranging such procedures, including responsibilities of the staff, informational flows, confidentiality of information, dissemination of information to the Authorized Body, and control over the system.
2. For the prevention of ML/TF, special attention should be paid to the following types of transactions (activities):
 - 1) Early terminated contracts, particularly:
 - a. Contracts with the same customer, providing for small commission fees and terminated on the same day before the end of the contract;
 - b. Contracts for which the refunded commission fees have been transferred to an account different from the one initially used for transactions;
 - c. Regular conclusions and early terminations of contracts with the same customer;
 - d. Other similar cases;
 - 2) Contracts providing for high commission fees;

- 3) Any other transaction (activity) which supervisors consider to be suspicious and (or) unusual.
3. Examine compliance of the investment company's policy for customer service, customer identification ("Know Your Customer"), scrutiny of high-risk transactions and/ or business relationships, and risk management with the standards practiced internationally and/ or adopted by the Authorized Body.
4. Get acquainted with the staff of the investment company's customer service for getting an idea about their professionalism and awareness in the applicable legislation on combating ML/TF and relevant internal regulatory acts.
5. Find out whether the investment company ensures confidentiality of information on suspicious transactions.
6. Discuss with the staff of the CBA Financial Monitoring Center the deficiencies identified due to the examination, the examiner's concerns about the investment company's practice in combating money laundering and terrorism financing.

Legal Compliance

Find out whether the requirements of the Law on Combating Money Laundering and Terrorism Financing and other legal statutes have not been violated in the course of combating ML/TF.

6.2.4. Procedure for Examining Internal Control

Appropriate Policy

47. Find out whether the investment company has internal procedures for defining a policy for combating ML/TF.
48. Find out whether the Internal Monitoring Unit regularly monitors effectiveness of implementation of the policy for combating ML/TF, makes recommendations on enhancing its effectiveness.
49. Find out whether the opinion of other stakeholders is taken into consideration while defining the policy for combating ML/TF.
50. Find out whether the policy for combating ML/TF, before being approved by the authorized governance body of the investment company, is checked for compliance with the requirements of current legislation.
51. Check whether the policy for combating ML/TF and the changes therein are approved by the authorized governance body of the investment company.
52. Find out whether the policy for combating ML/TF is regularly (at least once a year) revised to take into consideration the changes in the activities of the investment company, the principles set forth by involved international organizations, and the practical examples of ML/TF typologies.
53. Find out whether the investment company has clearly articulated internal procedures for the company's staff members and other stakeholders to make recommendations on necessary revisions of the policy for combating ML/TF.

Appropriate Application

1. Find out whether there are internal procedures to control implementation of the policy for combating ML/TF.
2. Find out whether the investment company at least once a year conducts internal audit to check appropriate performance of the duties stipulated by the Law on Combating Money Laundering and Terrorism Financing, by other legal statutes, and by the internal regulatory acts of the investment company.
3. Find out whether the Internal Audit regularly reports to the authorized governance body and the executive management body on its findings and disclosures, including its conclusions on the relevance and efficiency of the AML/CFT staff training and professional development.
4. Find out whether the investment company commissions external audit to check implementation and effectiveness of the legislation on combating money laundering and terrorism financing, in the manner established by the Authorized Body, upon the request of the Authorized Body or by their own initiative.
5. Find out whether there are mechanisms for imposing disciplinary sanctions on the company staff in case of violation of the policy for combating ML/TF.

Appropriate Recordkeeping

1. Find out whether the investment company has internal procedures for collecting, recording, and maintaining data on its customers, as well as on suspicious transactions (business relationships).
2. Find out whether the investment company's internal regulatory acts on recognizing suspicious transactions and business relationships and reporting to the Authorized Body provide for:
 - The procedures for communicating to the Internal Monitoring Unit the preliminary information (assumptions) on suspicious transactions or business relationships;
 - The rules and deadlines for the Internal Monitoring Unit to process, verify, and put forward possible conclusions on suspicious transactions or business relationships;
 - The possible actions and analyses for recognizing suspicious transactions or business relationships, including the access to national and international databases, the requests, the criteria for assessing their results, and the rules for summarizing such results.
3. Find out whether the Internal Monitoring Unit monitors recordkeeping and maintenance of information.
4. Find out whether the investment company has internal procedures for reporting to the Authorized Body.

Assessment of Risk

1. Find out whether there is an Internal Monitoring Unit or a staff member in the investment company engaged in combating money laundering and terrorism financing, or has this function been delegated to a specialized entity (hereinafter referred to as the Internal Monitoring Unit). In investment companies, the function of internal monitoring can not be assigned to a staff member of the customer service.

2. Find out whether the Internal Monitoring Unit is independent in performing its functions and has a status of senior management of the investment company.
3. Find out whether the investment company has operational procedures for the Internal Monitoring Unit.
4. Find out whether the Internal Monitoring Unit has direct access to all documents pertaining to concluded contracts and performed transactions, whether it is empowered to require clarifications from any staff member of other subdivisions on transactions and business relationships, as well as on customers, their authorized persons, and beneficial owners.
5. Find out whether the Internal Monitoring Unit reports to the authorized governance body of the investment company on the findings of the review and other issues raised by the Authorized Body
6. Find out whether the Internal Monitoring Unit makes the decision on suspending or rejecting a transaction or a business relationship, as well as on freezing terrorism-related funds.
7. Find out whether the staff of the Internal Monitoring Unit carries out appropriate and efficient analyses to recognize suspicious transactions and business relationships.
8. Find out whether the Internal Monitoring Unit oversees the ongoing monitoring of business relationships and periodically reviews the process of refining and updating available data; provides for the categorization of the investment company's customers based on the risk profile; carries out ongoing monitoring of high-risk business relationships.
9. Find out whether the investment company has a list of the documents and other information required for regular and enhanced due diligence.
10. Find out whether the investment company has internal procedures for suspending (rejecting) suspicious transactions (business relationships); freezing funds of terrorism-related persons.
11. Find out whether there is an appropriate system of control and monitoring so as to timely recognize suspicious transactions, and to file prompt and accurate reports with the Authorized Body.
12. Find out whether the investment company's internal regulatory acts provide for and apply relevant measures for counteracting money laundering or terrorism financing risks associated with new or developing technologies.
13. Find out whether the investment company's staff involved in the prevention of money laundering and terrorism financing is regularly trained on the matter of their duties and responsibilities; whether, in case of hiring new personnel, the investment company organizes trainings on combating money laundering and terrorism financing within the first three months of their employment.
14. Find out whether there a program for the professional development of the staff specifying the periodicity, themes, positions, and other pertinent minimal requirements with regard to training.
15. Find out whether there is designated staff in the investment company responsible for the organization and implementation of training programs.
16. Find out whether there are defined criteria for categorizing the customers based on the risk profile, and special rules are applied to high-risk customers.

17. Find out whether the investment company's internal regulatory acts require that, in the presence of high risk criteria, enhanced customer due diligence is performed.
18. While performing enhanced due diligence, does the investment company:
 - 1) Carry out more comprehensive and in-depth check of the veracity of the documents (information) required for establishing business relationships with the customer;
 - 2) Require information on the source of the customer's assets and other funds;
 - 3) Examine the information on the customer, the business relationship, and the transaction through various databases;
 - 4) Make requests to other reporting entities or to other bodies, including foreign counterparts, to check the information on the customer, on his business relationships and occasional transactions;
 - 5) Take other measures to get a comprehensive and full understanding of the customer, the transactions performed by him and the business relationships established with him.
19. Find out whether the investment company conducts additional scrutiny of all complex and unusually large transactions (business relationships), as well as of the ones involving unusual patterns with no apparent economic or other legitimate purpose.
20. Find out whether the investment company carries out regular analysis of the dynamics and risk profile of customer transactions; particularly to ensure that:
 - 1) The existing interrelation between the transactions, the possible schemes of such interrelations, as well as the objectives of the transactions are disclosed;
 - 2) The substance of the transactions corresponds to the type of activities performed by the customer;
 - 3) Possible information on the customer's sources of income is collected;
 - 4) The sources of funds, their movement and volumes of transaction are compared;
 - 5) The possible money laundering and terrorism financing risks pertinent to the transaction or business relationships are assessed by means of comparing them with the grounds and criteria of suspicious transactions and business relationships;
 - 6) It is checked whether there are business relationships and (or) occasional transactions, with which the customer aims to avoid being reported by the investment company to the Authorized Body;
 - 7) The types, periodicity, and chronology of the transaction within a certain period of time are checked;
 - 8) Data on transaction parties, recipients, beneficial owners, as well as on authorized persons is recorded and compared so as to identify interrelations between customers; and
 - 9) Other measures stipulated by the investment company's internal regulatory acts are performed.

Legal Compliance

Find out whether the Internal Monitoring Unit reviews the compliance of the investment company's transactions (business relationships), as well as of activities of its structural and territorial divisions and staff members with the Law on Combating Money Laundering and Terrorism Financing, with other normative legal statutes adopted on basis thereof, and with the internal regulatory acts, in the manner and at the periodicity established by the investment company's internal regulatory acts, but no less than once in every six months.

**ANNEX 31 - CENTRAL BANK OF ARMENIA BOARD DRAFT
DECISION ON MAKING AN AMENDMENT TO THE CENTRAL
BANK OF ARMENIA BOARD DECISION N 386-N, DATED JULY
29, 2005 ®**

Restricted