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

MONEYVAL (2010) 11

Montenegro

Progress report[1]

16 March 2010

[1] First 3rd Round Written Progress Report Submitted to MONEYVAL

Montenegro is a member of MONEYVAL. This progress report was adopted at MONEYVAL's 32nd Plenary meeting (Strasbourg, 15-18 March 2010). For further information on the examination and adoption of this report, please refer to the Meeting Report (ref. MONEYVAL(2010)13) 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).

LIST OF ACRONYMS

AML/CFT - Anti money laundering and counter terrorism financing
ANS – Agency for National Security
APMLTF – Administration for the Prevention of Money Laundering and Terrorist Financing
CAFAO – European Union Customs and Fiscal Assistance Office
CBM - Central Bank of Montenegro
CC – Criminal Code
CDA – Central Depository Agency
CDD - Customer Due Diligence
CPC – Criminal Procedure Code
CRPS – Central Register of the Commercial Court (CRCC)
DNFBP - Designated Non-financial Businesses and Professions
EBRD - European Bank for Reconstruction and Development
EU – European Union
EUR – Euro
FATF - Financial Action Task Force
FIU – Financial Intelligence Unit
GDP - Gross Domestic Product
IAIS – International Association of Insurance Supervisors
IPA - Instrument for Pre-accession Assistance
KZ CG – Criminal Code of Montenegro (CC of Montenegro)
LLC - Limited liability company
LPMLTF – Law on the Prevention of Money Laundering and Terrorist Financing
ML - Money Laundering
MoU – Memorandum of Understanding
MNE – Montenegro
MVT service - Money or Value Transfer services
NPO - Non-profit Organisations
NGO – Nongovernmental Organisations
OGM – Official Gazette of Montenegro
OSCE – Organisation for Development and co-operation in Europe
PEP – Politically Exposed Person
R – Recommendation
S/RES - Security Council Resolution
SR - Special Recommendation
STR- Suspicious Transaction Report
TF - Terrorist Financing
UN – United Nations

1. *General overview of the current situation and the developments since the last evaluation relevant in the AML/CFT field*

After the most important step that Montenegro has made in approaching the EU, on 15th December 2008, when it presented its official application for joining the EU, the European Council on 23rd March 2009 invited the European Commission to submit its opinion on the application. The next step was presenting Montenegro with the European Commission's Questionnaire on 22 July 2009, which formally represents the beginning of the procedure of deciding on accepting the candidacy of Montenegro for the EU membership. Montenegro officially sent the responses to the Questionnaire on 9 December 2009, and the set of responses to the additional questions were sent to the EC at the end of January 2010.

By the Council of European Union decision the nationals of Montenegro can as of 19th December 2009 travel without visas to the EU countries and to the three countries that are not EU members, but have accessed the Schengen area (Switzerland, Norway and Island). The requirement needed for entering the mentioned countries is to own biometric passports that have been issued in Montenegro since 5th May 2008. The decision on visa liberalization refers to entrance and stay up to 90 days within six months, with the purpose of tourist visit, business stay, visit to cousins and friends, business meetings and similar.

The NATO Ministers of Foreign Affairs, in the meeting held on 4th December 2009 in Brussels, took a decision on Montenegro's joining the Membership Action Plan (MAP) – a NATO program of assistance and practical support tailored to the individual needs of countries wishing to join the Alliance.

The activities for implementing the strategic commitments of Montenegro for the EU membership, within the accession process, are targeted at further meeting of obligations undertaken by signing the Stabilization and Association Agreement and the Interim Agreement on trade and trade-related matters between the European Community and Montenegro, as well as by the tasks set in the National Program for Integration with the European Union for the period 2008 – 2012, and the obligations that will follow depending on the forthcoming accession phases.

Considering the strategic documents, in the period following the last evaluation, in March 2009, the Government of Montenegro made a decision to develop, for the forthcoming three-year period, a **Strategy for Fight against Corruption and Organised Crime** and the **Action plan** for the implementation of the Strategy, and the drafting of these documents is underway. The working group formed by the Minister of Interior Affairs and Public Administration is composed of the representatives of the following institutions: Ministry of Interior Affairs and Public Administration, Ministry of Justice, Ministry of Finance, Prosecutor's Office, judiciary, Police Directorate, Directorate for Anti-Corruption Initiative, Administration for the Prevention of Money Laundering and Terrorist Financing, State Audit Institution, Customs Administration, Department of Public Revenues and two NGOs. This group has begun the activities related to the drafting of the mentioned documents. Namely, on 28th July 2005, the Government of Montenegro adopted the **Program of Fight against Corruption and Organised Crime**, as the first national strategic document that has defined the goals that are to be reached in the area of fight against organised crime and corruption.

With a view to implementing the measures defined in this Program, the Government of Montenegro has adopted on 24th August 2006 the **Action Plan for the implementation of the Program of Fight against Corruption and Organised Crime**. The National Commission for monitoring the implementation of the Action Plan for the implementation of the Program of Fight against Corruption and Organised Crime was established on 15th December 2007. On 29th May 2008 the **Innovated Action Plan for the implementation of the Program of Fight against Corruption and Organised Crime for the period 2008 - 2009** was adopted. The realisation of measures and activities defined in the Innovated Action Plan

for the implementation of the Program of Fight against Corruption and Organised Crime was planned to be completed till 31st December 2009. Thus the Government of Montenegro passed a decision to develop a **Strategy for Fight against Corruption and Organised Crime and the Action plan for the implementation of the Strategy for the forthcoming three-year period, from 2010 to 2012**.

The activities related to drafting the national **Strategy for Fight against Terrorism, Money Laundering and Terrorist financing** and the **Action Plan for the implementation of the Strategy for the period 2009 – 2012**. An interagency Working Group for drafting the Bill for these documents was formed. The members of the Working Group are the representatives of the following institutions: Ministry of Interior Affairs and Public Administration, Prosecutor's Office, Central Bank of Montenegro, Insurance Supervision Agency, the Ministry of Finance, the Ministry of Justice, the Customs Administration, Police Directorate, Directorate for Anti-Corruption Initiative, Administration for Games on Chance, Securities Commission, Administration for the Prevention of Money Laundering and Terrorist Financing, National Security Agency, State Audit Institution and the representatives of the non-governmental sector.

The Working group, composed of the representatives of: Administration for the Prevention of Money Laundering and Terrorist Financing, Police Directorate, Department of Public Revenues, Customs Administration, with the help of the OSCE Mission to Montenegro Customs and Fiscal Assistance Office – CAFAO, United Nations Office on Drugs and Crime – UNODC, Swedish National Police Board, International Criminal Investigative Training Assistance Program – ICITAP, US Embassy and British Embassy, harmonised the model of joint office for coordination and intelligence data exchange- with working title " National coordination office for the state administration". The establishing of this office will enable data exchange between the Administration for the Prevention of Money Laundering and Terrorist Financing, the Police Directorate, the Department of Public Revenues and the Customs Administration.

On 28th January 2009, the Central Bank of Montenegro and the European Central Bank concluded the agreement of co-operation and exchange of information, through which CBM joined the efforts undertaken by the ECB in the field of prevention and detection of false euro banknotes.

On 7th May 2009, the Central Bank of Montenegro and the National Bank of Serbia signed the Protocol on business co-operation in the field of professional improvement of employees.

On 16th October 2009, the Central Bank of Montenegro and the Croatian National Bank signed Memorandum of Understanding establishing the co-operation in supervising banks operating in the territory of the Republic of Montenegro and the Republic of Croatia.

In the period from the last evaluation in March 2009 Montenegro has largely progressed in harmonisation of criminal legislation with the European standards – through adoption of the new Criminal Procedure Code, and drafting of the Law on Amendments of the Criminal Code.

In July 2009 the new Criminal Procedure Code was adopted („Official Gazette of Montenegro" 57/2009). In the newly adopted Code, special attention was dedicated to confiscation of revenues, property and material gain acquired through criminal act. The Code, in Article 90, stipulates the procedure for temporary confiscation of property and financial investigation for expanded confiscation of property. Through adoption of this Code the procedure of permanent confiscation of property whose legal origin was not proven is introduced (Art. 486-489). The procedure stipulates that after the irrevocability of the judgment by which the accused is pronounced guilty for a criminal act for which the Criminal Code stipulates the possibility of expanded confiscation of property from the convicted, his legal successor or the person to whom the convicted transferred the property, who can not prove the legality of its origin, the state prosecutor, within the period of one year the latest, submits a request for permanent confiscation of

the property of the convicted, his legal successor or the person to whom the convicted transferred the property for which he can not prove the legality of its origin. The request is submitted to the convict without delay, to his legal successor or the person to whom the convicted transferred the property, with the warning that he is obliged to prove the legality of the origin of the property, and that the property will be confiscated if the legality of its origin is not proved. If the convicted, his legal successor or the person to whom the convicted transferred the property, by valid documents, or in the absence of valid documents, in another way does not prove the legality of the origin of the property, the court reaches a decision on permanent confiscation of the property. If the convicted, his legal successor or the person to whom the convicted transferred the property, by valid documents, or in the absence of valid documents, in another way proves the legality of the origin of the property or a part of the property, the court reaches a decision on complete or partial dismissal of the request for permanent confiscation of the property.

Provisions of the Criminal Procedure Code relating to temporary confiscation of property and financial investigation for expanded confiscation of property (art. 90) and the procedure of permanent confiscation of property whose legal origin was not proved (art. 486-489) start to be applied from the day of beginning of the application of the provisions of the Law on Amendments of the Criminal Code. The procedure of adopting of this law is in progress. The new solutions will, through adopting of the instrument of expanded confiscation of property gain and reverse burden of proof and in material-legal sense, enable their application stipulated by the procedural law.

According to the Article 158 of the new Criminal Procedure Code, it is prescribed the list of the criminal offences for which is possible to order measure of secret surveillance. Montenegro has accepted recommendation of MONEYVAL- to have the possibility to order those measures for types of the criminal offence – money laundering, which recommendation was given in the Third round of mutual evaluation on Montenegro. In the previous CPC measures of secret surveillance could be ordered only for the criminal offences punishable by minimum of 10 years of imprisonment as well as for the criminal offences committed in the organised way, so measures of secret surveillance, according to this previous Code, could be ordered only if the money laundering was committed in the organised way. In order to avoid this kind of limitation, new Criminal Procedure Code prescribes in article 158:

Measures of secret surveillance may be ordered for the following criminal offence:

1. For which a prison sentence of ten years or more serve penalty may be imposed
2. Having elements of organised crime
3. Having elements of corruption, as follows: money laundering, causing false bankruptcy, abuse of assessment, passive bribery, active bribery, disclosure of an official secret, trading in influence, abuse of authority in economy, abuse of an official position and fraud in the conduct of official duty with prescribed imprisonment sentence of eight year or more
4. Abduction, extortion, blackmail, mediation in prostitution, displaying pornographic material, usury, tax and contributions evasion, smuggling, unlawful processing, disposal and sorting of dangerous substances, attack on a person acting in an official capacity during performance on an official duty, obstruction of evidences, criminal association, unlawful keeping of weapons and explosions, illegal crossing of the state border and smuggling in human being
5. Against the security of computer data

A great step forward was taken also in view of amendments of incriminations of criminal offences of money laundering and terrorist financing, in accordance with the recommendations of FATF, relevant conventions of the Council of Europe, the United Nations and *acquis communautaire*. These amendments introduce criminal offences of abuse of authority in business activities and unlawful influence – which

could be predicate for money laundering offence – as recommended after the evaluation of MONEYVAL. A significant novelty is also incorporation of the new criminal offence of forming a criminal organisation (Article 401a) within the criminal acts against public peace and order. It relates to incrimination that will enable a more efficient and stricter criminal-legal intervention regarding the organised crime offences. The term and conditions of criminal organisation are given in accordance with the UN Convention on trans-national organised crime. With this Law, in the chapter of criminal offences against humanity and other goods protected by international law several amendments were conducted, and the most significant are the ones starting from the new concept of terrorist offences.

The basic terrorism offence (regardless whether the act is directed against Montenegro, a foreign state or an international organisation) is stipulated in Article 447 with many forms of committing an offence. This criminal offence, as well as new terrorist offences such as public calling to commit acts of terrorism (Article 447a CC), incitement and training to commit acts of terrorism (Article 447b CC), use of lethal device (Article 447c CC), destruction and damage of nuclear object (Article 447d CC), endangering of persons under international protection (Article 448), as well as terrorist financing (Article 449) were included and brought in line with a number of conventions aiming at prevention of terrorist acts, and specially with the Convention of the Council of Europe on the Prevention of Terrorism from 2005 that was ratified by Montenegro in 2008.

In the framework of those changes, the definition of the criminal offence – money laundering is now completely in accordance with Vienna and Palermo Conventions.

In the field of international judiciary co-operation, it is important to point out that after the accession of Montenegro to the Convention of the Council of Europe on Laundering, Search, Seizure and Confiscation of Proceeds from Crime and on the Financing of Terrorism (CETS 198), in December 2009 Montenegro accessed to another important convention in the field of international legal assistance – European Convention on Mutual Assistance in Criminal Matters with additional protocols, European Convention on Extradition with additional protocols and European Convention on Transfer of Convicted Persons with additional protocols, by confirming this convention Montenegro completed the set of international instruments applied in the area of international legal assistance in criminal matters.

In accordance with the National Program for Integration of Montenegro into the EU, adoption of the law that will define appliance and implementation of the restrictive measures, competences of certain state authorities and manner of record keeping on natural and legal person against whom international restrictive measures are introduced, or the law by which the legal framework for introducing unilateral restrictive measures will be created, is planned for the end of 2011.

Supreme State Prosecutor's Office, according to the Law on Amendments and Changes of the Law on State Prosecutors, extended the competences of the Department for suppression of organised crime corruption, terrorism and war crime. The Department is now competent for the criminal offences of corruption, terrorism, and war crime

On September 15th 2008, the number of deputies of prosecutors in the Department has been extended. Now in the Department for suppression of organised crime corruption, terrorism and war crime there are Special Prosecutor and five Deputies, and the Department has the adequate premises and techniques.

During 2009, on the basis of the Law on the Prevention of Money Laundering and Terrorist Financing (Official Gazette of Montenegro No. 14/07 from 21.12.2007) in addition to:

i.)„The Rulebook on the Manner of Work of the Compliance Officer, the Manner of Conducting the Internal Control, Data Keeping and Protection, Manner of Record Keeping and Employees' Professional Training" (Official Gazette of Montenegro No. 80 of 26. 12. 2008) and

ii.) The Rulebook on the Manner of Reporting Cash Transactions in the Amount of 15,000 Euros and more and Suspicious Transactions to the Administration for the Prevention of Money Laundering and Terrorist Financing (Official Gazette of Montenegro No. 79 of 23.12.2008),

the following were passed as well:

- **„The Rulebook on Developing Risk Analysis Guidelines with a view to Preventing Money Laundering and Terrorist Financing„ (Official Gazette of Montenegro No. 20/09 of 17.03.2009)**
- **„The Rulebook on Indicators for recognising Suspicious Clients and Transactions„ (Official Gazette of Montenegro No. 69/09 of 16.10.2009)** determines the List of Indicators. The List of Indicators for recognising suspicious customers and transactions is included in the Rulebook, as follows:

  - List of Indicators for banks,
  - List of Indicators for capital market,
  - List of Indicators for the Customs Administration,
  - List of Indicators for the Department of Public Revenues,
  - List of Indicators for leasing companies,
  - List of Indicators for auditors,
  - List of Indicators for accountants,
  - List of Indicators for lawyers and
  - General indicators.

On the basis of the Rulebook on Developing Risk Analysis Guidelines with a view to Preventing Money Laundering and Terrorist Financing (Official Gazette of Montenegro No. 79 20/09 of 17.03.2009), the APMLTF has determined the Guidelines on developing risk analysis with a view to preventing money laundering and terrorist financing for the reporting entities the APMLTF supervises (the reporting entities from the Article 4 Paragraph 2 items 14 and 15 of the LPMLTF).

Guidelines were also determined by the following supervising authorities: the Securities Commission and the Administration for Games on Chance. The guidelines of the Central Bank of MNE are in the draft form.

Regarding the bilateral co-operation with the counterparts from other countries, during 2009 the APMLTF signed several Memoranda of Understanding – financial intelligence data exchange with: FIC EULEX – Kosovo, the State Committee for Financial Monitoring (FIU) of Ukraine, as well as with the Anti-money Laundering and Suspicious Cases Unit – United Arab Emirates FIU and the Financial Intelligence Agency - FIA Bermuda.

Securities Commission has concluded several bilateral agreements with international supervisors of securities market in relation with co-operation and exchanging data . On 17th February 2009 Securities

commission signed IOSCO Multilateral Memorandum of Understanding Concerning Consultation and Co-operation and the Exchange of Information

Supreme State Prosecutor's Office and Police Directorate concluded the Memorandum of Understanding and exchange of information related to prevention, detection and prosecution of offenders prosecuted ex officio.

On 19th February 2010 APMLTF, Supreme State Prosecutor's Office, Police Directorate Department of Public Revenues and Customs Administration signed the MoU in prevention and prosecution of offenders related to organised crime and corruption

The MoU defines obligations, general rules and terms of forming and working of the joint team that will act in special cases of organised crime and corruption. The team, whose work will be coordinated by the Supreme State Prosecutor, is composed of representatives of APMLTF, Supreme State Prosecutor's Office, Police Directorate Department of Public Revenues and Customs Administration, who will be appointed for the period of three years..

On the national level, the APMLTF signed the Memorandum of Understanding with the State Audit Institution of Montenegro in March 2009.

On the basis of analysing the assessment of needs for concluding new bilateral Memoranda, the APMLTF has, for the forthcoming period, planned signing memoranda with those supervising authorities from Article 86 of the LPMLTF with which it has not signed memoranda yet, as well as innovating the previously signed memoranda.

With a view to implementing the MONEYVAL experts' recommendations related to changes in the national legislation in the AML/CFT area, the Ministry of Finance has, upon the initiative of the APMLTF, started the activities for preparing the changes of the LPMLTF. The working group, formed by the Ministry of Finance (which proposes the law), consists of the representatives of the following institutions: Ministry of Finance, Administration for the Prevention of Money Laundering and Terrorist Financing, legislative authorities, Ministry of Justice, Ministry of Interior Affairs and Public Administration and the Administration for Games on Chance. The working group will, when drafting the changes to the Law, be introduced to all the MONEYVAL experts' recommendations referring to the solutions in the LPMLTF, in order to meet all the criteria from the FATF Recommendations. The Government of Montenegro adopts the Proposal for changing. Afterwards, the Proposal is subject to parliamentary procedure, relevant parliamentary boards' consideration, parliamentary discussion and adoption.

According to its competencies to participate in professional training and improvement of the compliance officers at reporting entities, APMLTF organised a two-day Workshop for reporting entities' compliance officers on the subject „Preventing money laundering and terrorist financing in the financial and non-financial sector". The participants were representatives of various categories of reporting entities: commercial banks, brokers, car dealers, leasing companies, casinos, real estate agencies...

With a view to effectively implementing the LPMLTF and bylaws, in the forthcoming period, the APMLTF will:

- *Strengthen institutional co-operation with other institutions involved in AML/CFT system;* (APMLTF has been planning to sign Memoranda of Understanding with other supervising authorities from Article 86 of the LPMLTF, as well as to innovate some previously signed Memoranda of Understanding with Customs Administration, Department of Public

Revenues, Ministry of Interior Affairs, Central Bank of Montenegro, Securities Commission and Basic Court in Podgorica).

- *Improve international co-operation with the competent institutions of other countries (*signing Memoranda of Understanding with several more countries, as well as innovating some of the already signed Memoranda are being planned).

- *Improve the existing IT system;* (In order to fully implement the new data delivery forms which make an integral part of the Rulebook on the Manner of Reporting Cash Transactions in the Amount of 15,000 Euros and more and Suspicious Transactions, APMLTF will initiate a complete innovation of the existing IT system. Supplying the special analytical software I2 and the training for designers and users of this software are underway).

- *Proceed with continuous training of professionals;* (APMLTF will proceed with organising trainings for reporting entities compliance officers and the employees that directly contact with customers. The training will be focused on more effective implementation of the Law and bylaws, with special reference to PEPs, proper identification, recognition and reporting of suspicious transactions to the APMLTF on the basis of STR indicators, ML typologies...).

As a regulatory authority of the insurance market, the Insurance Supervision Agency is involved in the implementation of measures from the innovated action plan for the implementation of programs against the corruption and organised crime, among which is one of the tasks that the Agency undertook by this plan. The task is establishing guidelines on risk analysis to prevent money laundering and terrorism financing, and defining other procedures aimed at identifying suspicious transactions, and that will be addressed to obligators under Article 4, paragraph 8 of the Law on Prevention of money laundering and terrorism financing, i.e. insurance companies and branches of foreign insurance companies that conduct life insurance business. The above mentioned guidelines will be harmonised with the Regulation on the development of guidelines for risk analysis to prevent money laundering and financing terrorism, adopted by the Ministry of Finance during the 2009 year.

Activities on the development of these Guidelines, Agency began at the beginning of the 2010 and it is expected that the activities of their development and publishing will be completed in the first half of this year. Also, those activities began within the IPA 2008 twinning project "Strengthening the regulatory and supervisory capacity of financial regulators", whose goal is aid to the financial regulators in Montenegro in building institutional capacity through the technical assistance and professional training of employees, establishing a modern operational procedures, strengthening co-operation between financial regulators and ensuring greater stability of the entire financial system. The start of the activities is expected at the end of January 2010 under the fourth component within the mentioned project, which is related to the Insurance Supervision Agency. One of the activities will refer to the preparation / review of appropriate guidelines for addressed reporting entities who are defined by the existing Law on AML/CFT, and that project activity will be the best control done so far regarding this issue. The ultimate goal of this part of the project will be transposing the European legislation from this area into National legislation as well as adaptation of the function of supervision of the Agency in accordance with the best international practice from this area.

In the previous period, co-operation with the authorities involved in the system AML/CFT was successful and comprehensive. However, in accordance with the conclusions of the Government of Montenegro, the Insurance Supervision Agency is planning to formalize mentioned co-operation's during 2010 through the special agreements on co-operation signed from the both sides.

Since its recent establishment, the priority of the Agency in 2009 was the establishment of co-operation and signing formal agreements with the insurance market regulators and institutions from the Region, as well as those on the global level. In 2009, the Agency has become a full member of the International Association of the Insurance Supervisors - IAIS, which will significantly facilitate the establishment of closer level of co-operation and exchange of information of the Agency with the insurance regulators in the world, efficient monitoring and improving the overall financial stability in Montenegro. With the same goal, but in the regional framework, during 2009 the Agency has achieved intensive co-operation and contacts with all the insurance regulators in the Region. Formal Memorandums of Understanding were signed with the Austrian Financial Market Authority - FMA, Insurance Supervision Agency of Slovenia and the Croatian Agency for Supervision of Financial Services - HANFA.

In order to strengthen its institutional capacity, the Agency has recently started with the activities in this field. Within the IPA 2007 twinning project "Fight against organised crime and corruption", employees of the Agency have participated in training in the period from 30.08 to 04.09.2009, which was provided by the representatives of the administration of the United Kingdom and Northern Ireland, and dedicated to representatives of the supervisory authority under the Law of AML/CFT.

Throughout the already mentioned fourth component of the IPA 2008 twinning project, during 2010 and the beginning of the 2011, it will be implemented a range of activities with the goal to improve existing legislation in the field of AML/CFT, building professional capacity of the Agency regarding AML/CFT, raising the legal awareness of Law reporting entities and public opinion, as well as improving co-operation between supervisory authorities in the field. Quoted will include the analysis of the current regulatory framework, preparing the draft guidelines which will be used in this area by the Agency, developing programs and techniques of inspections for the Agency, as well as providing training to the addressed reporting entities defined by the Law of AML/CFT. It also includes preparation of informational materials, raising awareness about the importance of AML/CFT among the competent bodies which are connected by the Law of AML/CFT, prosecution and judiciary, and, at the end, eventually establishing formal co-operation between supervisory authorities, or more precisely, signing the Memorandums of Understanding.

2. *Key recommendations*

Please indicate improvements which have been made in respect of the FATF Key Recommendations (Recommendations 1, 5, 10, 13; Special Recommendations II and IV) and the Recommended Action Plan (Appendix 1).

Recommendation 1 (Money Laundering offence)	
Rating: PC	
Recommendation of the MONEYVAL Report	*The money laundering offence as defined by the Criminal Code is basically sound, but it lacks further refinement; the current formulation of criminalized behaviour (conversion/transfer and concealment/disguise) is narrower than the requirements in the Vienna and Palermo Conventions and should be clarified in the Criminal Code.*
Measures taken to implement the Recommendation of the Report	At the moment of completing the Progress Report for Montenegro, the Law on Amendments of the Criminal Code of Montenegro is in the adoption procedure. Review of the criminal legislation is conducted within a comprehensive reform of the judicial system in Montenegro, in accordance with the Judicial Reform Strategy 2007-2012 and the Action Plan for Implementation of the Judicial Reform Strategy

	2007-2012 which stipulates it as a measure of amendments to the Criminal Code in view of harmonisation with the international standards, primarily the European Union, the United Nations and the Council of Europe. Also, the National Program for Integration of Montenegro into the European Union stipulates as a short-term priority the harmonisation of the Criminal Code with international standards in the part of "Judiciary and Fundamental Rights". In reviewing of the Criminal Code, special accent was placed at harmonisation with the standards in the field of fight against organised crime, corruption and terrorism, and specially through complex changes of the definition of these criminal offences and adoption of the instrument of expanded confiscation of material gain acquired through criminal offence and the reverse burden of proof of legality of property acquisition, which is stipulated also with the newly adopted Criminal Procedure Code. With the new solutions in the Criminal Code, in accordance with the recommendations of the MONEYVAL Committee, the definition "Money laundering" offence from Article 268 was amended. With the aim of complete harmonisation with the solutions stipulated by the Vienna and Palermo Convention, the new definition in the Criminal Code abolishes the limitation of money laundering offence as business activity that included "banking, financial and other business operation". Also, in accordance with the recommendations, every form of replacement (conversion) and transfer, as well as acquiring, keeping and use of money or other property acquired through criminal offence was incorporated in the definition of the money laundering offence. Concealment and false presentation of facts on the nature, origin, place of depositing, movement, disposal or possession of money or other property acquired through criminal offence was also incriminated. In accordance with the Vienna and Palermo Convention, with the amendments of the Criminal Code, this offence was incriminated in the following way: ***„Money laundering*** ***Article 268*** *(1) Anyone who conducts conversion or transfer of money or other property knowing it was obtained through a criminal act, with the intent to conceal or falsely present the origin of money or other property, or anyone who acquires, keeps or uses money or other property knowing at the moment of reception that it was obtained through a criminal act, or anyone who conceals or falsely presents facts on the nature, origin, place of depositing, movement, disposal or possession of money or other property knowing it was obtained through a criminal act,* *shall be punished by an imprisonment sentence of six months to five years* *(2) If the offender committing an act as of Paragraph 1 of this Article is at the same time a perpetrator or an accomplice in a criminal act through which money or property gain as of Paragraph 1 of this Article is obtained, s/he shall be punished by a sentence from paragraph 1 of this article.* *(3) If the amount of money or the value of property referred to in Paragraphs 1 and 2 of this Article exceeds forty thousand Euros, the offender shall be punished by an imprisonment sentence for a term of one to ten years* *(4) If an act referred to in Paragraphs 1 and 2 of this Article is committed by more persons who joined together to commit such acts, they shall be punished by an imprisonment sentence of three to twelve years.* *(5) Anyone who commits the act referred to in Paragraphs 1 and 2 of this Article and he could have known or ought to have known that money or property represent income gained by criminal activity, shall be punished by imprisonment for a term of*

	up to three years. *(6) Money and property as of Paragraphs 1, 2 and 3 of this Article shall be confiscated."* This definition of the criminal offence–money laundering has completely eliminated limitations that this criminal offence can only be committed by bank, financial or other type of business operation, and any type of conversion or money transfer was not incriminated.
(Other) changes since the last evaluation	Through amendments of the Criminal Code, in accordance with the tendency of complete harmonisation with the international standards and in the corpus of criminal offences against humanity and other goods protected by international law, several amendments were conducted, and the most significant are the ones that come from the new concept of terrorist offences. The basic terrorist criminal offence (regardless of whether the offence was directed against Montenegro, a foreign country or an international organisation) is stipulated in Article 447 with numerous forms of acts of commission. This criminal offence, as well as the new terrorist criminal offences such as public calling to commit acts of terrorism (Article 447a CC), incitement and training to commit acts of terrorism (Article 447b CC), use of lethal device (Article 447c CC), destruction and damage of nuclear object (Article 447d CC), endangering of persons under international protection (Article 448), as well as financing of terrorism (Article 449) were included and brought in line with a number of conventions aiming at prevention of acts of terrorism, and specially with the Convention of the Council of Europe on the Prevention of Terrorism from 2005 that was ratified by Montenegro in 2008. These amendments also expanded Article 447 of the Criminal Code „international terrorism“. In the old definition of this article the criminal offence of international terrorism would be performed by a person who with the intent to harm a foreign country or an international organisation, abducts a person or commits some other violence, causes explosion or fire or commits other generally dangerous acts or threatens to use nuclear, chemical, bacterial or other similar means. With the new definition in this article, with the aim of broader incrimination, from the title of this article the prefix "international" was removed and terrorism against the interest of the citizens, Montenegro, other states and international organisations (thus both domestic and international) was included. The criminal offence upon adoption of the Law on amendments of the Criminal Code will be as follows: ***"Terrorism*** ***Article 447*** *(1) Anyone who with the intent to seriously intimidate the citizens or to compel Montenegro, a foreign country or an international organisation to do/to abstain from doing, or to seriously endanger or harm the basic constitutional, political, economic or social structures of Montenegro, a foreign country or an international organisation, commits one of these acts:* *1) attack to life, body or freedom of another,* *2) abduction or hostage taking,* *3) destruction of state and public objects, transport systems, infrastructure including information systems, immovable platforms in the epicontinental area, general goods or private properties that can endanger lives of people or cause significant damage for economy,* *4) abduction of aircraft, ship, means of public transport or transport of goods that can endanger the life of people,* *5) production, possession, obtaining, transport, supply or use of weapons, explosives, nuclear or radioactive material or devices, nuclear, biological or*

chemical weapons,
6) research and development of nuclear, biological or chemical weapons,
7) release of dangerous materials and causing fires, explosions or floods or committing other generally dangerous act that can endanger the life of people,
8) obstruction or cessation of supplying water, electricity or other energy that can endanger the life of people,
shall be punished by an imprisonment sentence of minimum five years.
(2) Anyone who threatens to commit a criminal act referred to in Paragraph 1 of this Article,
shall be punished by an imprisonment sentence of six months to five years.
(3) If an offence referred to in Paragraph 1 of this Article resulted in death of one or more persons or caused great destructions, the offender shall be punished by an imprisonment sentence for a term of minimum ten years.
(4) If in the commission of crime referred to in Paragraph 1 of this Article the offender has committed a premeditated murder of one or more persons, the offender shall be punished by an imprisonment for a minimum term of twelve years or by an imprisonment of forty years."

Also, after Article 447 with the new Law four new articles are added Article 447 a, 447 b, 447 c i 447 d as follows:

*"**Public calling to commit acts of terrorism***
Article 447a
Anyone who publically calls or in other way incites to commit a criminal act referred to in Article 447
shall be punished by an imprisonment sentence for a term from one to ten years.

Incitement and training to commit acts of terrorism
Article 447b
(1) Anyone who with the intent of committing an act referred to in article 447 of this code, incites another person to commit or participate in commission of that act or to join a group of people or a criminal association in order to participate in commission of that criminal act,
shall be punished by an imprisonment sentence for a term of one to ten years.
(2) Anyone who with the intent of committing an act referred to in article 447 of this code, gives instructions on creation and use of explosive devices, fire or other arms or harmful or dangerous materials or trains another person to commit or participate in commission of that criminal act shall be punished by a sentence referred to in paragraph 1 of this article.

Use of lethal device
Article 447c
(1) Anyone who with the intent of murdering another person, inflicts a heavy bodily injury or destroys or significantly damages state or public facility, system of public transport or another facility that has greater significance for security or supplying of citizens or for economy or for functioning of public services, makes, transfers, keeps, gives to another person, puts up or activates a lethal device (explosive, chemical means, biological means or poisons or radioactive means) in a public place or in an facility or next to that facility,
shall be punished by an imprisonment sentence of one to eight years.
(2) If in the commission of crime referred to in Paragraph 1 of this Article, the

	offender has committed a premeditated severe bodily injury or destroyed or significantly damaged a facility, *he/she shall be punished by an imprisonment sentence of five to fifteen years.* *(3) If in the commission of crime referred to in Paragraph 1 of this Article, the offender has committed a premeditated murder of one or more persons,* *he/she shall be punished by an imprisonment sentence of minimum ten years or an imprisonment sentence of fourteen years.* ***Destruction and damage of nuclear facility*** ***Article 447d*** *(1) Anyone who with the intent to murder another person, inflicts severe bodily injury, endangers environment or inflicts significant property damage, destroys or damages a nuclear facility in the manner that releases or there is a possibility to release radioactive material,* *shall be punished by an imprisonment sentence of two to ten years.* *(2) If in commission of an act referred to in paragraph 1 of this article, offender inflicts a premeditated severe bodily injury or destroys or significantly damages a nuclear facility,* *he/she shall be punished by an imprisonment sentence of five to fifteen years.* *(3) If in commission of an act referred to in paragraph 1 of this article, offender committed a premeditated murder of one or more persons,* *he/she shall be punished by an imprisonment sentence of minimum ten years or an imprisonment sentence of fourteen years."* And Article 448 „Hostage taking“ is changed and is as follows: *" **Endangering persons under international protection*** ***Article 448*** *(1) Anyone who conducts abduction or some other act of violence upon a person under international legal protection,* *shall be punished by an imprisonment sentence of two to twelve years.* *(2) Anyone who violates official premises, a private apartment or a means of transport of a person under international legal protection, in the manner that endangers his/her security and personal freedom,* *shall be punished by an imprisonment sentence of one to eight years.* *(3) If an act referred to in Paragraphs 1 and 2 of this Article resulted in death of one or more persons, the offender shall be punished by an imprisonment sentence of five to fifteen years.* *(4) If in commission of an act referred to in Paragraphs 1 and 2 of this article, the offender committed a premeditated murder of a person,* *he/she shall be punished by an imprisonment sentence of minimum ten years or an imprisonment sentence of fourteen years* *(5) Anyone who endangers security of persons referred to in Paragraph 1 of this Article by a serious threat to attack him/her, his/her official premises, private apartment or a means of transport, shall be punished by an imprisonment sentence of six months to five years."* Amendments of Article 449 – "Financing of terrorism", will be described in the answer relating to implementation of the Special Recommendation II.

Recommendation of the MONEYVAL Report	*The Criminal Code should be amended to clearly include insider trading and market manipulation offences as predicate offences for money laundering.*
Measures taken to implement the Recommendation of the Report	In accordance with the recommendations, the Criminal Code was amended by stipulating the insider trading and market manipulation as criminal offences, which in accordance with the „all crimes approach“ can now be predicate offences for money laundering offence. The criminal act of "Negligent performance of business activities " from Article 272, in accordance with the recommendations, is amended and shall be as follows: ***"Abuse of authority in business activities*** ***Article 272*** *(1) A responsible person in a company, some other economic entity or other legal person who by abuse of his/her authority or trust in view of disposing of another persons property, exceeding the limits of his/her authorisation or non-performance of his/her duty obtains for him/herself or for another person unlawful property gain or causes property damage,* *shall be punished by an imprisonment sentence of three months to five years.* *(2) Anyone who obtains for him/herself or for another person unlawful property gain, appropriates money, securities or other movables entrusted to him/her for work in the company, other economic entity or another legal person shall be punished by a sentence referred to in Paragraph 1 of this Article.* *(3) If through an act referred to in Paragraphs 1 and 2 of this Article material gain exceeding the amount of forty thousand Euros is obtained, the perpetrator shall be punished by an imprisonment of two to ten years."* Criminal offence of „Illegal mediation“ from Article 422, in accordance with the recommendations, was amended and shall be as follows: ***"Unlawful influence*** ***Article 422*** *(1) Anyone who demands or accepts a reward or any other material benefit or accepts promise of reward or other benefit for himself or another person by taking advantage of his official or social position or influence for interceding that an official act be or not be performed, shall be punished by imprisonment for a term of three months to three years.* *(2) Anyone who, by taking advantage of his official or social position or influence, intercedes that an official act that should not be performed be performed or that an official act that should be performed not be performed, shall be punished by imprisonment for a term of six months to five years* *(3) If a reward or any other benefit has been received for intercession referred to in Paragraph 2 of this Article,* *the offender shall be punished by imprisonment for a term of one to eight years.* *(4) The reward and material gain shall be confiscated."* The amendments stipulate adding of a new article 422^a – where soliciting to unlawful influence, by giving, offering or promising reward is also stipulated as a criminal offence. This article is as follows:

	"Incitement to unlawful influence ***Article 422a*** *(1) Anyone who offers or promises to a person acting in an official capacity or another person a reward or any other benefit for interceding that an official act be or not be performed by taking advantage of his official or social position or influence,* *shall be punished by imprisonment for a term of up to two years.* *(2) Anyone who offers or promises to a person acting in an official capacity or another person a reward or any other benefit for interceding that an official act that should not be performed be performed or that an official act that should be performed not be performed by taking advantage of his official or social position or influence,* *shall be punished by imprisonment for a term of three months to three years.* *(3) Perpetrator of an act referred to in Paragraphs 1 and 2 of this Article who reported the act before he found out that it was revealed can be acquitted.* *(4) The reward and material gain shall be confiscated."* In both articles relating to the insider trade – unlawful influence from Art. 422 and incitement to unlawful influence from Art. 422[a], a measure of mandatory confiscation of the reward and material gain is stipulated. Through entering into force of this Law, these two offences stated in the recommendations of the committee will also be predicate for money laundering offence, in accordance with the Convention on Laundering, Search, Seizure and Confiscation of Proceeds from Crime and Financing of Terrorism.
Recommendation of the MONEYVAL Report	*There is relatively strict regulation of extraterritoriality in the case of offences committed by persons who are not citizens of Montenegro against a foreign state. This also raises the question of inclusion of "all serious offences" in the predicate offences. This is subject to incriminations in those countries and if offences are not punishable with at least 5 years imprisonment, the offence would not be considered a predicate offence in Montenegro. Abolition of this limitation (5 years imprisonment) would prevent such situations.*
Measures taken to implement the Recommendation of the Report	We are in the process of the reform of the criminal material law, and this recommendation of MONEYVAL was presented to the working group in order to have complete compliance of our law with the international standards. With the Law on amendments to the Criminal Code which is in adoption procedure, provisions relating to the validity of the criminal legislation of Montenegro were also amended. In Article 135 relating to validity of the criminal legislation of Montenegro for perpetrators of certain criminal offences committed abroad, the validity of criminal legislation of Montenegro was expanded (apart from the committed criminal offences from the corpus of offences against constitutional order and safety of Montenegro and money forgery offences from Art. 258) and the persons who conduct criminal offences 447,448, and 449 abroad, which are in accordance with the amendments stipulated as terrorism, endangering of persons under international protection and financing of terrorism.
(Other) changes since the last evaluation	

<table>
<tr><th colspan="2">Recommendation 5 (Customer due diligence)
I. Regarding financial institutions</th></tr>
<tr><td colspan="2">Rating: PC</td></tr>
<tr><td>Recommendation of the MONEYVAL Report</td><td>It is the view of the evaluators that the wording of the second point under Article 9 is too precise and could be interpreted to read that only transactions of exactly €15,000 require CDD. The evaluators consider that <u>”or more”</u> should be added in Article 9, Paragraph 1 number 2 in the LPMLTF.</td></tr>
<tr><td>Measures taken to implement the Recommendation of the Report</td><td>Upon the APMLTF initiative, the Ministry of Finance has started the activities on preparing the Bill on Changes and Amendments to the LPMLTF in accordance with this and other recommendations from the MONEYVAL’s Recommended action plan, in order to make the changes and amendments of the LPMLTF fully complied with the international standards, so that the Law would completely satisfy all the needed criteria from FATF Recommendations. The Minister of Finance has formed a working group responsible for preparing the Bill on Changes and Amendments to the LPMLTF. Members of the working group are the representatives of the relevant state authorities: Ministry of Finance, APMLTF, legislative authorities, Ministry of Justice, Ministry of Interior Affairs and Administration for Games on Chance.

The Securities and Exchange Commission, for the purpose of implementation of its obligations under LPMLTF considers that the wording of the second point of the article 9 implies that the 15.000€ requirement is the lowest amount required for notification, and that each transaction that overcomes the 15.000€ threshold should be reported. In that aim, the Securities and Exchange Commission in Article 4 of the Instruction on risk analysis of money laundering, „know your client” procedures and other procedures for recognising suspicious transactions prescribed:
“Capital market participant is obliged to verify the identity of the client, gather data about customer and transaction (hereinafter: identification) according to the regulation on combating money laundering, especially in following cases:
a) opening owners securities account securities or establishing of some other kind of business relations with the client;
b) of one or more linked transactions amounting to € 15. 000 <u>or the higher amount</u>;
c) with every transaction, irrespective of value of such transaction when there are reasonable grounds for suspicion of money laundering in regard to transaction or a client”.</td></tr>
<tr><td>(Other) changes since the last evaluation</td><td>This Recommendation was implemented by the Instruction of the Securities and Exchange Commission even prior the last evaluation.</td></tr>
<tr><td>Recommendation of the MONEYVAL Report</td><td>The LPMLTF should be amended to require CDD to be conducted on wire transactions of €1,000 or more.</td></tr>
<tr><td>Measures taken to implement the Recommendation of the Report</td><td>The members of the Working Group will be presented with all the MONEYVAL expert’s recommendations for changing and amending the LPMLTF.
Securities brokers do not conduct cash transactions, but only transactions where money is transferred from client’s account within the bank to brokers account specified for keeping client’s money. However, the securities brokers are required to perform CDD even though they are not receiving money for performing transactions in cash from the clients. The specific obligations of the securities brokers regarding CDD are imposed by the Securities and Exchange Commission Instruction.</td></tr>
</table>

(Other) changes since the last evaluation	This Recommendation was implemented by the Instruction of the Securities and Exchange Commission even prior the last evaluation
Recommendation of the MONEYVAL Report	*The LPMLTF should be amended to require reporting entities to verify that persons purporting to act on behalf of a customer have the authority to act on behalf of the customer. Article 15 of the LPMLTF should be amended to require the obtaining of copies of the document regulating the power to bind the legal person or arrangement.*
Measures taken to implement the Recommendation of the Report	The response is the same as the one given to the previous question. The Securities and Exchange Commission adopted Rules on Conduct of Business of Licensed Market Participants that are published in the Official Gazette of Montenegro ("Official Gazette of Montenegro", No. 78/09 and 87/09) that precisely prescribe the obligation of the licensed market participants to verify identity of persons acting of behalf of clients and to obtain originals or certified copies of the documents authorising them to act on their behalf. The article 4 paragraph 3 of the Rules explicitly states: “Licensee may conclude the contract on providing securities services and/or accept an order for buying or selling of securities on the basis of power of attorney, if a power of attorney was issued and verified in accordance with the Law.” Furthermore, the article 5, paragraphs 2,3, and 4 explicitly state: “Identity verification of a legal entity presupposes verification of the identity of a person authorised for its representation. If a client is represented by a proxy, his/her power of attorney must be certified by a competent authority. Original power of attorney or documentation proving status of a legal proxy or guardian, shall remain in a file at licensee’s office.” Also, the abovementioned is included in the article 11 paragraph 2 of *Instruction on risk analysis of money laundering, „know your client” procedures and other procedures for recognising suspicious transactions* which is adopted by the Securities and Exchange Commission and prescribes: When establishing business relationship or executing transaction by proxy or authorised person (agent) on client’s behalf, capital market participants are obliged to identify authorised person, (agent, attorney) and a client on whose behalf the account has been opened or transaction executed, solely on the basis of personal and another public certificate such as: – Certificate properly issued by state body within their own competence, or institution or other legal entity within legally entrusted public authority and – Written authorisation- power of attorney, certified by notary, consulate, court or state administration body.
(Other) changes since the last evaluation	Rules on Conduct of Business of Licensed Market Participants that are published in the Official Gazette of Montenegro ("Official Gazette of Montenegro", No. 78/09 and 87/09).
Recommendation of the MONEYVAL Report	*The problem of reliance on certificates from the commercial register for CDD purposes should be addressed by establishing procedures to address the limitations of the commercial register.*
Measures taken to implement the Recommendation of the Report	The Securities and Exchange Commission does not authorise licensed market participants to rely on the electronic version of Commercial Register for CDD purposes due to fact that the such verification is not updated on real time basis. The Securities and Exchange Commission prescribes in the article 6 paragraph 4 of

	the Rules on Conduct of Business of Licensed Market Participants that are published in the Official Gazette of Montenegro ("Official Gazette of Montenegro", No. 78/09 and 87/09) that legal entity should be indentified on the basis of original statement from the registry of Commercial court. The Securities and Exchange Commission Rules prescribe obligation of the licensed market participant to make a suspicious transaction report in circumstances where they have been unable to conduct satisfactory CDD. Also, the Rules authorise securities participants to withdraw from the contract and to reject acceptance of the client's order if they have any suspicion about money laundering (Article 19par.6 item 4). Furthermore, the Instruction in the article 6 par. 5 and 6 prescribe: " If an reporting entity, when establishing and verifying the identity of a customer, doubts the accuracy of obtained data or veracity of documents and other business files from which the data have been obtained, he shall request a written statement from the agent or authorised person before establishing business relationship or executing a transaction. Capital market participant may refuse to establish business relationship with the client or executing of such transaction, if regardless of taking measures from this article, there are still serious doubts about identity of the beneficial customer." Separate clause is inserted into the Instruction of Securities and Exchange Commission requiring capital market participant to specifically deal with the issue of CDD on existing customers. The Article 7 of the abovementioned Instruction explicitly states obligation of the licensed market participants to take following procedures: a) before establishing business relationship or executing transaction determine and verify the identity of a client and identity of beneficial owner on the basis of documents, data and information enabling determination of the identity in doubtless and assertive way; b) taking measures enabling checking and determining ownership structure of the client and real control over the client in order to determine identity of the beneficial owner client; c) obtain and keep data and documents in order to establish identity and risk factor of a customer; d) constantly monitor business relationship with the client, including transaction during that relationship (are they adjusted to the kind of business and risks regarding client and information about that customer) keeping records on monitoring business relationship; e) If possible, before establishing business relationship with the client, establish reasons for terminating contracts with other participant on the capital market; f) During executions transactions of customer who is identified with technology help that not include direct contact, enforce procedures that enable previous authenticity checks verity of instruction transaction and authenticity of their applicators.
(Other) changes since the last evaluation	Rules on Conduct of Business of Licensed Market Participants that are published in the Official Gazette of Montenegro ("Official Gazette of Montenegro", No. 78/09 and 87/09).
Recommendation of the MONEYVAL Report	*Article 29.4 of the LPMLTF appears to go further than intended by Criteria 5.9 in that it permits simplified customer verification in respect of customers to "whom an insignificant risk of money laundering or terrorist financing is related" which could include a broader range of customers than those envisaged in Criteria 5.9. Article 29.4 should be amended to bring it into line with the essential criteria.*

Measures taken to implement the Recommendation of the Report	The Securities and Exchange Commission adopted abovementioned Instruction prior to enactment of the Rulebook on making Guidelines for risk analysis with the aim of combating money laundering and terrorist financing ("Official Gazette of Montenegro", No. 20/09). The Instruction of the Securities and Exchange Commission thus does not provide for any exceptions of the general rule that customers and clients are subject to complete CDD procedures nor provide for reduced or simplified CDD measures to be applied. Also, this Rulebook does not provide for any exceptions and Securities and Exchange Commission is not required to provide for it by Instruction that is adopts. The Bill on Changes and Amendments to the LPMLTF will include this recommendation as well.
Recommendation of the MONEYVAL Report	*The FATF definition ("Beneficial owner refers to the natural person(s) who ultimately owns or controls a customer and/or the person on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate effective control over a legal person or arrangement.") should be incorporated into the LPMLTF and a requirement to identify and verify the "ultimate" beneficial owner should be included.*
Measures taken to implement the Recommendation of the Report	Article 19 of the LPMLTF defines a beneficial owner: "In the context of this Law the following shall be considered as a beneficial owner of a business organisation or legal person: 1. a natural person who indirectly or directly owns more than 25% of the shares, voting rights and other rights, on the basis of which he/she participates in the management, or owns more than a 25% share of the capital or has a dominating influence in the assets management of the business organisation, and 2. a natural person that indirectly ensures or is ensuring funds to a business organisation and on that basis has the right to influence significantly the decision making process of the managing body of the business organisation when decisions concerning financing and business are made. Also, a business organisation, legal person, as well as an institution or other foreign legal person that is directly or indirectly a holder of at least €500,000 of shares, or capital share, shall be considered a foreign owner. As a beneficial owner of an institution or other foreign legal person (trust, fund and the like) that receives, manages or allocates assets for certain purposes, in the context of this Law, shall be considered: 1. a natural person, that indirectly or directly controls more than 25% of a legal person's asset or of a similar foreign legal entity, and 2. a natural person, determined or determinable as a beneficiary of more than 25% of the income from property that he/she manages." Article 10 of the LPMLTF defines that a reporting entity, when establishing a business relationship with a customer shall: 1. identify a customer and beneficial owner if the customer is a legal person: 2. obtain and verify data on a customer, or beneficial owner, if the customer is a legal person, on the purpose and nature of a business relationship or transaction and other data pursuant to this Law, and 3. monitor regularly the business activities that a customer undertakes with the reporting entity and verify their compliance with the nature of a business relationship and the usual scope and type of customer's affairs. Under Article 20 of the LPMLTF a reporting entity shall establish the beneficial owner of a legal person or foreign legal person by obtaining data from Article 71 item 15 of this Law (name, address of permanent residence or temporary residence,

	date and place of birth of the beneficiary owner- legal person or in case from the Article 19 paragraph 2 item 2 of this Law, data on the category of the person, on whose behalf is establishing and operating of the legal person or similar foreign legal person). A reporting entity shall obtain these data by checking the original or certified copy of the documentation from the CRCC or other appropriate public register that may not be older than three months of its issue date or obtain them on the basis of the CRCC or other public register in accordance with Article 14 paragraphs 3 and 5 of this Law. If the required data cannot be obtained in the manner determined in paragraphs 1 and 2 of this Article, an reporting entity shall obtain the missing data from a written statement of an agent or authorised person. Data on beneficial owners of a legal person or similar foreign legal entity shall be verified to the extent that ensures complete and clear insight into the beneficial ownership and managing authority of a customer respecting risk-degree assessment. Moreover, under Art. 21 of the LPMLTF, within the customer due diligence, a reporting entity shall, - when establishing business relationship, obtain the data from Art. 71 items 1, 2, 4, 5, 7, 8 and 15 (name, address of permanent residence or temporary residence and the birth date and birth place of the beneficial owner of a legal person, or in the case from Art. 19 paragraph 3 item 2 of the Law, obtain the data on the category of the person, on whose behalf is the establishing and operating of the legal person or similar foreign legal person) of this Law. - when one or several linked transactions in the amount of €15.000 are executed, obtain data from Art. 71 items 1, 2, 3, 4, 5, 9, 10, 11, 12 and 15 (name, address of permanent residence or temporary residence and the birth date and birth place of the beneficial owner of a legal person, or in the case from Art. 19 paragraph 3 item 2 of the Law, obtain the data on the category of the person, on whose behalf is the establishing and operating of the legal person or similar foreign legal person) of this Law. - from Art. 9 paragraph 1 items 3 and 4 of the Law/(3) when there is a suspicion about the accuracy or veracity of the obtained customer identification data; 4) when there are reasonable grounds to suspect that a transaction or customer are related to ML and TF, obtain data from Art. 71 of this Law (which includes item 15 referring to beneficial owner). Art. 22 /Monitoring business activities/, defines the following: "An reporting entity shall monitor customer's business activities, including the sources of funds the customer uses for business, in order to identify the customer more easily. Monitoring business activities from paragraph 1 of this Article at an reporting entity shall particularly include the following: 1. verifying the compliance of customer's business with nature and purpose of contractual relationship; 2. monitoring and verifying the compliance of customer's business with usual scope of her/his affairs, and 3. monitoring and regular updating of documents and data on a customer, which includes conducting repeated annual control of a customer in the cases from Article 24 of this Law. An reporting entity shall ensure and adjust the dynamics of undertaking measures from paragraph 1 of this Article to the risk of money laundering and terrorist financing, to which an reporting entity is exposed when performing certain work or

	when dealing with a customer."
Recommendation of the MONEYVAL Report	*Article 25 of the LPMLTF is very specific and does not cover a number of the specified categories as set out in Criteria 5.8, namely all non-resident customers, private banking, legal persons or arrangements such as trusts that are personal assets holding vehicles and companies that have nominee shareholders or shares in bearer form. The evaluators consider that the LPMLTF should be amended to fully reflect all of the categories in Criteria 5.8.*
Measures taken to implement the Recommendation of the Report	In Montenegro trusts may not be formed. The legal persons or practitioners may just register companies, but may not as a way of business form companies or other legal persons, act or arrange for another person to act as a director or secretary of a company; as a partner of a partnership; in a similar position in relation to other legal persons; provide a registered office, business address, correspondence or administrative address or other related services for a company, partnership or any other legal person or arrangement, act or arrange for another person to act as: (i) a trustee of an express trust or similar legal arrangement (ii) a nominee shareholder for another person other than a company listed on a regulated market which is subject to disclosure requirements consistent with Community legislation or equivalent international standards; The Working Group that will prepare the changes and amendments to the LPMLTF will be presented with this MONEYVAL recommendation as well.
Recommendation of the MONEYVAL Report	*Risk guidelines in accordance with Criteria 5.12 should be completed and published.*
Measures taken to implement the Recommendation of the Report	The Ministry of Finance adopted, "The Rulebook on Developing Risk Analysis Guidelines with a view to Preventing Money Laundering and Terrorist Financing" (Official Gazette of Montenegro No. 20/09 of 17.03.2009). APMLTF has determined the Guidelines on Developing Risk Analysis with a view to Preventing Money Laundering and Terrorist Financing for the reporting entities that are supervised by APMLTF. The Guidelines define specific risk factors used as basis for establishing the degree of risk of customers, group of customers, business relationship, transaction or product. The Guidelines are applicable since 25th September 2009. On the basis of the Guidelines, the reporting entities from Art. 4 paragraph 2 it. 14 and 15 of the LPMLTF, will, according to the provisions of Art. 8 paragraph 1 of the LPMLTF, make risk analysis in order to determine the risk assessment of groups of customers or of an individual customer, business relationship, transaction or product related to the possibility of misuse for the purpose of money laundering or terrorist financing. The APMLTF Guidelines are given in the ANEX of this Report. The Securities and Exchange Commission has issued Instruction of the Securities and Exchange Commission of on risk analysis of money laundering, „know your client" procedures and other procedures for recognising suspicious transactions of November 28, 2008. This Instruction has been adopted before last evaluation. The Instruction implements the Rulebook on developing risk analysis guidelines with a view to preventing money laundering and terrorist financing. The Administration for the games on chance adopted on 25th December 2009, the Guidelines on developing risk analysis with a view to preventing money laundering and terrorist financing and forwarded it to the organisers of the games of chance that

	are supervised by the Administration. The Guidelines are given in the Annex of this Report. Pursuant to Article 86 of the LPMLTF (OGM 14/07 4/08) the Central Bank of Montenegro supervises the enforcement of this law by the reporting entities specified under Article 4 paragraph 1 points 1, 2, 3, 10 and 13, these being banks and foreign bank branches, savings banks and savings credit organisations, payment system organisations, exchange offices, and electronic money institutions. In line with Article 8 paragraph 3 of the LPMLTF, the Ministry of Finance passed the Rulebook on the development of guidelines on risk analysis with a view to preventing money laundering and terrorism financing (OGM 20/09) providing for detailed criteria for drafting the guidelines by the authorities specified under Article 86 of the LPMLTF. The Central Bank of Montenegro has prepared the Draft Guidelines on bank risk analysis aimed at preventing money laundering and terrorism financing to be adopted by the Council of the Central Bank of Montenegro. The Draft Guidelines above are attached hereof. We underline that the 5.12 criteria standards are covered in the Draft Guidelines. At the beginning of 2010, the ISA has started with the activities concerning preparation of risk analysis Guidelines regarding prevention of money laundering and terrorist financing, based on which reporting entities defined by the Law on PML/CFT and which are under the scope of ISA, will be obliged to make their internal procedures in this field. This work will be finished, at latest, by the end of the 6th month of 2010.
Recommendation of the MONEYVAL Report	*A specific clause should be inserted into the LPMLTF requiring reporting entities to consider making a suspicious transaction report in circumstances where they have been unable to conduct satisfactory CDD. Likewise there should also be a clause requiring reporting entities to terminate a business relationship in circumstances where they have been unable to conduct satisfactory CDD. This is particularly relevant in circumstances where CDD has not been possible for existing customers where there are one or more linked transactions amounting to €15,000, etc..*
Measures taken to implement the Recommendation of the Report	The above clauses are inserted into Securities and Exchange Commission Rules on Conduct of Business of Licensed Market Participants that are published in the Official Gazette of Montenegro ("Official Gazette of Montenegro", No. 78/09 and 87/09) The Securities and Exchange Commission Rules prescribe obligation of the licensed market participant to make a suspicious transaction report in circumstances where they have been unable to conduct satisfactory CDD. Also, the Rules authorise securities participants to withdraw from the contract and to reject acceptance of the client's order if they have any suspicion about money laundering (Article 19 par.6 item 4). Furthermore, the Instruction in the article 6 par. 5 and 6 prescribe: " If an reporting entity, when establishing and verifying the identity of a customer, doubts the accuracy of obtained data or veracity of documents and other business files from which the data have been obtained, he shall request a written statement from the agent or authorised person before establishing business relationship or executing a transaction. Capital market participant may refuse to establish business relationship with the client or executing of such transaction, if regardless of taking measures from this article, there are still serious doubts about identity of the beneficial customer." The Bill on Changes and Amendments to the LPMLTF will include this recommendation as well.

(Other) changes since the last evaluation	Rules on Conduct of Business of Licensed Market Participants that are published in the Official Gazette of Montenegro ("Official Gazette of Montenegro", No. 78/09 and 87/09)
Recommendation of the MONEYVAL Report	*There needs to be a specific requirement for reporting entities to assess and consider the risks of technological developments as part of their risk analysis. This should also be introduced in the guidelines to be produced by the supervisory bodies.*
Measures taken to implement the Recommendation of the Report	Banks are obliged to assess and consider the risk of technology development which should be an integral part of a comprehensive analysis of the risk that could arise from money laundering and terrorism financing. Therefore, in its Draft Guidelines on bank risk analysis, chapter 3 paragraph 4, the Central Bank of Montenegro has defined the following: "With a view to ensuring a proper risk management in the area of preventing money laundering and terrorism financing, a bank shall reduce its exposure to risk arising from new technologies providing anonymity (electronic or internet banking, electronic money, etc.), i.e. the bank is obliged to define in its policies and procedures in particular, but not limited to the following: • identification of the party using electronic banking services; • authenticity of the signed electronic document; • reliable measures against the forgery of documents and signatures; • systems ensuring and enabling safe electronic banking; • other requirements in accordance with positive regulations governing the aforesaid business area." The Securities and Exchange Commission implemented this recommendation by the article 22 par. 6-9 of the Rules on Conduct of Business of Licensed Market Participants that are published in the Official Gazette of Montenegro ("Official Gazette of Montenegro", No. 78/09 and 87/09). These Rules specifically regulate the procedures to be followed by the licensed market participants if the client uses electronic means of communication to submit an order or conclude a contract. "Client, who gives orders by phone, fax or electronically, may give the same with authorisation by identity code which licensee shall assign to a client when signing a contract. A client is obliged to keep his/her identity code as a secret, and may not make it available to third persons. Licensee is obliged to check client's identity through identity code, contained in any contract prescribing possibility of submitting orders by phone, fax or electronically or in any other manner which does not imply client's face to face transaction. When prescribing possibility of electronic submitting of client's orders, licensee is obliged to provide: - reliable manner of client identification; - that all necessary elements of an order are stated in the electronic message; - a record of exact time when the order arrived to an e-mail and time of its entry in the order book; - sending of reply to a received order, where the original message of order sender is clearly visible; When prescribing possibility of electronic submitting of client's orders, licensee shall retain the right to refuse order execution, if the order is unclear and/or ambiguous, and he/she shall inform a client on that in the same way it accepted an

	order." This condition will be an integral part of already mentioned risk analysis Guidelines.
(Other) changes since the last evaluation	Rules on Conduct of Business of Licensed Market Participants that are published in the Official Gazette of Montenegro ("Official Gazette of Montenegro", No. 78/09 and 87/09)
Recommendation of the MONEYVAL Report	*It is the view of the evaluators that the requirements of Criteria 5.17 are essentially met although the wording of the first point above is too precise and could be interpreted to read that only transactions of exactly €15,000 require CDD. Furthermore, the requirement is for CDD to be conducted when "a transaction of significance takes place." and in the context of Criteria 5.17 it is considered that this is more appropriate wording. Overall the evaluators consider that a separate clause should be inserted into the LPMLTF to specifically deal with the issue of CDD on existing customers.*
Measures taken to implement the Recommendation of the Report	The Bill on Changes and Amendments to the LPMLTF will include this recommendation as well. Art. 23 of the applicable LPMLTF determines the repeated annual control: "If a foreign legal person executes transactions from Article 9 paragraph 1 of this Law at an reporting entity, the reporting entity shall, in addition to monitoring business activities from Article 22 of this Law, conduct repeated annual control of a foreign legal person at least once a year, and not later than after the expiry of one year period since the last control of a customer. By the way of exception to paragraph 1 of this Article an reporting entity shall, at least once a year, and not later than after the expiry of one year period since the last control of a customer, also conduct repeated control when the customer executing transactions from Article 9 paragraph 1 of this Law is a legal person with a registered office in Montenegro, if the foreign capital share in that legal person is at least 25%. Repeated annual control of a customer from paragraphs 1 and 2 of this Article shall include: 1.obtaining or verifying data on the company, address and registered office; 2.obtaining data on personal name and permanent and temporary residence of an agent; 3.obtaining data on a beneficial owner, and 4.obtaining a new power of authorisation from Article 17 paragraph 2 of this Law. If the business unit of a foreign legal person executes transactions from Article 9 paragraph 1 of this Law on behalf and for the account of a foreign legal person, an reporting entity, when conducting repeated control of a foreign legal person, in addition to data from paragraph 3 of this Article, shall also obtain: 1.data on the address and registered office of the business unit of a foreign legal person, and 2.data on personal name and permanent residence of the agent of the foreign legal person business unit . An reporting entity shall obtain the data from paragraph 3 items 1, 2 and 3 of this Article by checking the original or certified copy of the documentation from the CRCC or other appropriate public register that may not be older than three months of its issue date, or by checking the CRCC or other appropriate public register. If the required data cannot be obtained by checking the documentation, the missing data shall be obtained from the original or certified copy of documents and other business files, forwarded by a legal person upon an reporting entity's request, or directly from a written statement of the agent of a legal person from paragraphs 1 and 2 of this

	Article. By the way of exception to paragraphs 1, 2, 3, 4 and 5 of this Article an reporting entity shall conduct repeated control of a foreign person from Article 29 item 1 of this Law.”
(Other) changes since the last evaluation	

Recommendation 5 (Customer due diligence) **II. Regarding DNFBP[1]**	
Rating: PC	
Recommendation of the MONEYVAL Report	*Trust and Company Service Providers should be designated as obliged parties.*
Measures taken to implement the Recommendation of the Report	In Montenegro trusts may not be formed. The legal persons or practitioners may just register companies, but may not as a way of business form companies or other legal persons, act or arrange for another person to act as a director or secretary of a company; as a partner of a partnership; in a similar position in relation to other legal persons; provide a registered office, business address, correspondence or administrative address or other related services for a company, partnership or any other legal person or arrangement, act or arrange for another person to act as: (i) a trustee of an express trust or similar legal arrangement(ii) a nominee shareholder for another person other than a company listed on a regulated market which is subject to disclosure requirements consistent with Community legislation or equivalent international standards; Art. 4 paragraph 3 of the LPMLTF defines that in addition to the reporting entities listed in Art 4 paragraph 2, the regulation of the Government of MNE can define other reporting entities that shall undertake AML/CFT measures if, considering the nature and manner of carrying out activities or business, there is a more significant risk of money laundering or terrorist financing.
(Other) changes since the last evaluation	
Recommendation of the MONEYVAL Report	*For casinos, CDD should be required above the €3,000 threshold.*
Measures taken to implement the Recommendation of the Report	Further Amendments on Law on the Prevention of Money Laundering and Terrorist Financing will include that provision.
(Other) changes since the last evaluation	
Recommendation of the MONEYVAL	*There should be a clear requirement for casinos to link the incoming customers to individual transactions.*

[1] i.e. part of Recommendation 12.

Report	
Measures taken to implement the Recommendation of the Report	According to the article 45 paragraph 4 of Law on Games of Chance („Official Gazette of Montenegro“, No. 52/04 and 13/07) the concessionaire must provide non stop audio-video surveillance of the casino with recording, this ensuring an on-going direct supervision and that means clients and their transaction can be monitored while watching recorded tapes.
(Other) changes since the last evaluation	
Recommendation of the MONEYVAL Report	*Effective systems for monitoring and ensuring compliance with CDD requirements across most of the DNFBP sectors need to be developed.*
Measures taken to implement the Recommendation of the Report	Art. 86 of the LPMLTF defines that the supervision of implementation of this Law and regulations passed on the basis of this Law, within the established jurisdiction, is carried out by: 1)<u>The Central Bank of Montenegro</u> over the following reporting entities: banks and foreign banks' branches and other financial institutions; savings-banks, and savings and loan institutions; organisations performing payment transactions; exchange offices; institutions for issuing electronic money; 2)<u>The Agency for Telecommunication and Postal Services</u> over post- offices; 3) <u>Securities Commission over</u>: companies for managing investment funds and branches of foreign companies for managing investment funds; companies for managing pension funds and branches of foreign companies for managing pension funds; stock brokers and branches of foreign stock brokers; 4) <u>Insurance Supervision Agency</u> over: insurance companies and branches of foreign insurance companies dealing with life assurance; 5) <u>Administration for Games on Chance,</u> through compliance officer, under the law regulating inspection, over organisers of lottery and special games of chance; 6) <u>Department of Public Revenues</u> over pawnshops; 7) <u>Ministry of Finance</u> over: audit companies, independent auditor and legal or natural persons providing accounting and tax advice services; 8) <u>Administration for the Prevention of Money Laundering and Terrorist Financing</u>, through an authorised person, under the law regulating inspection, over: humanitarian, nongovernmental and other non-profit organisations; 15) other business organisations, legal persons, entrepreneurs and natural persons engaged in an activity or business of: - sale and purchase of claims; - factoring; - third persons' property management; - issuing and performing operations with payment and credit cards; - financial leasing; - travel organisation; - real estate trade; - motor vehicles trade; - vessels and aircrafts trade; - safekeeping; - issuing warranties and other guarantees; - crediting and credit agencies; - granting loans and brokerage in loan negotiation affairs; - brokerage or representation in life insurance affairs, and

	- organising and conducting biddings, trading in works of art, precious metals and precious stones and precious metals and precious stones products, *as well as other goods*, when the payment is made in cash in the amount of € 15.000 or more, in one or more interconnected transactions. According to the LPMLTF and new APMLTF Job Positions Systematization and Organisation Act, the Reporting Entities Control Department was established, with a view to ensuring consistent implementation of LPMLTF by the reporting entities (Art. 4 paragraph 2 it. 14 and 15 LPMLTF). The measures undertaken by this Department are, besides the LPMLTF, as the basic Law, also defined by the Law on Inspection and the Law on Misdemeanors. The APMLTF signed the agreement on mutual co-operation with the following national institutions • Ministry of Internal Affairs – 23 July 2004 • Department of Public Revenues – 5th October 2004 • Customs Administration – 20th October .2004 • Basic Court in Podgorica -19th July 2005 • The Central Bank of Montenegro - 13th April 2006 • The Central Bank of Montenegro ; • Securities Commission -21st June 2006. MoUs signed with the competent state authorities enclose details and special conditions referring to the manner of mutual co-operation and exchanging data between APMLTF and the competent state authorities. Also, the MoUs include data that are usually exchanged in accordance with the LPMLTF, bylaws and internal acts of the signatories. Depending on the competencies of the particular state authority MoUs are composed in accordance with its competencies.
Recommendation of the MONEYVAL Report	*DNFBPs need to be made aware of their obligations regarding PEPs. Specific guidelines, aimed at DNFBPs should be developed. It is also recommended that a training programme be undertaken concerning the risks and controls necessary concerning dealings with politically exposed persons.*
Measures taken to implement the Recommendation of the Report	On the basis of the Guidelines, determined by APMLTF, the reporting entities from Art. 4 paragraph 2 it. 14 and 15 of the LPMLTF, will, according to the provisions of Art. 8 paragraph 1 of the LPMLTF, make risk analysis in order to determine the risk assessment of groups of customers or of an individual customer, business relationship, transaction or product related to the possibility of misuse for the purpose of money laundering or terrorist financing. The APMLTF Guidelines are given in the ANNEX of this Report. APMLTF organised a two-day Workshop for reporting entities' compliance officers on the subject „Preventing money laundering and terrorist financing in the financial and non-financial sector". The participants were representatives of various categories of reporting entities: commercial banks, brokers, car dealers, leasing companies, casinos, real estate agencies... The Guidelines for developing risk analysis, determined by the APMLTF, together with the Questionnaire for Identifying PEPs were presented at the Workshop. The Guidelines were also published on the APMLTF web site. In order to strengthen its institutional capacity, the Agency has recently started with the activities in this field. Within the IPA 2007 twinning project "Fight against organised crime and corruption", employees of the Agency have participated in training in the period from 30.08 to 04.09.2009, which was provided by the representatives of the administration of the United Kingdom and Northern Ireland, and dedicated to representatives of the supervisory authority under the Law of

	AML/CFT.
Recommendation of the MONEYVAL Report	*A requirement should be introduced for DNFBPs to have policies in place to prevent the misuse of technological developments in ML/TF.*
Measures taken to implement the Recommendation of the Report	Further Amendments on Law on the Prevention of Money Laundering and Terrorist Financing will include that provision
Recommendation of the MONEYVAL Report	*More attention need to be given to raising awareness and enforcing compliance in casinos*
Measures taken to implement the Recommendation of the Report	The Guidelines on risk analysis are written and forwarded to all operators of the games of chance on the territory of Montenegro
(Other) changes since the last evaluation	

Recommendation 10 (Record keeping) **I. Regarding Financial Institutions**	
Rating: LC	
Recommendation of the MONEYVAL Report	*There is no requirement that transaction records should be sufficient to permit reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of criminal activity in accordance with the requirements of essential criteria 10.1.1. The LPMLTF should be amended to take this requirement into account.*
Measures taken to implement the Recommendation of the Report	The Securities and Exchange Commission prescribes this requirement explicitly. This requirement is imposed by the article 38 of the Rules on Conduct of Business of Licensed Market Participants that are published in the Official Gazette of Montenegro ("Official Gazette of Montenegro", No. 78/09 and 87/09). The article states: "This information shall be entered in a manner that all transactions can be easily identified at any time, as well as a manner to easily track transaction from the time of initial order entry to final transaction;"
(Other) changes since the last evaluation	Rules on Conduct of Business of Licensed Market Participants that are published in the Official Gazette of Montenegro ("Official Gazette of Montenegro", No. 78/09 and 87/09).

Recommendation 13 (Suspicious transaction reporting) **I. Regarding Financial Institutions**	
Rating: PC	
Recommendation of the MONEYVAL Report	*The reporting obligation should be extended to include money laundering reporting obligations if the transaction has already been performed.*
Measures taken to implement the Recommendation	The Central Bank of Montenegro, by applying good practices, demands from banks to inform the Administration for the Prevention of Money Laundering and Terrorism Financing on any suspicious transaction (regardless of the amount and type) also

of the Report	after its execution. The Bill on Changes and Amendments to the LPMLTF will include this recommendation as well.
Recommendation of the MONEYVAL Report	*The Book of Rules should be endorsed in law with sanctions for breaches in order to become "other enforceable means".*
Measures taken to implement the Recommendation of the Report	The Law prescribes that the implementing regulations (rulebooks, decrees..) shall be adopted six months after the date the Law entered into force. **Drafting Regulations Rules (Official Gazette MNE, No.02/10 from 18.01.2010)** define the legal and technical rules for drafting laws and other regulations, as well as other enactments whose preparation, proposal and adoption are within the competence of the Government of Montenegro and Ministries, in order to ensure the uniformity in drafting regulations, to avoid legal and technical omissions and to accelerate the adoption procedure. 1.1. When drafting a law and determining its contents and scope, and elaborating the constitutional principles, it is important to distinguish between the issues that can be regulated only by law and those that can be regulated by other regulations and general enactments. 1.2. The contents of a law are classified by systematization of provisions according to what they are related to: a. General Provisions b. Main provisions c. Penalty provisions d. Transitional provisions e. Final provisions If the law prescribes that certain questions shall be regulated by several different bylaws and other laws (ex. Decrees and rulebooks…), special attention has to be paid to defining the issues that should be regulated by a single enactment, in order to ensure the harmonisation of these enactments according to their hierarchy and to avoid repetitions. **B. Drafting bylaws** A bylaw cannot contain the same provisions as law. A bylaw is composed of: a. Preamble b. Title c. Contents of the enactment d. Signature of the responsible person e. The number under which the enactment is recorded at the authority that adopted it and the date of adoption. Consequently, only law includes penalty provisions.
(Other) changes since the last evaluation	

Recommendation 13 (Suspicious transaction reporting) II. Regarding DNFBP[2]	
Rating: NC	
Recommendation of the MONEYVAL Report	*The obligation to report suspicious transactions that have been performed should be explicitly provided for in either law or regulation.*
Measures taken to implement the Recommendation of the Report	The Bill on Changes and Amendments to the LPMLTF will include this recommendation as well
(Other) changes since the last evaluation	

Special Recommendation II (Criminalisation of terrorist financing)	
Rating: PC	
Recommendation of the MONEYVAL Report	*A definition of "funds", which includes "assets of every kind, whether tangible or intangible, movable or immovable, however, acquired, and legal documents or instruments in any form, including electronic or digital, evidencing title to, or interest in, such assets, including, but not limited to, bank credits, travellers cheques, bank cheques, money orders, shares, securities, bonds, drafts, letters of credit." should be laid down in the Criminal Code.*
Measures taken to implement the Recommendation of the Report	In compliance with the Special Recommendation II of the Financial Action Task Force (FATF), "financing of terrorism" is defined as a separate criminal offence in the current Criminal Code of Montenegro ("Official Gazette of the RMNE" 70/03, 13/04, 47/06 and "Official Gazette of Montenegro" 40/08). The criminal offence of "Financing of Terrorism" (Article 449) is done by a person who provides or collects funds intended for financing execution of criminal offences of terrorism, international terrorism and taking of hostages. All the forms of criminal activity mentioned above are defined as separate criminal offences (Articles 365, 447 and 448 of the Criminal Code). Imprisonment for the period of one to ten years is prescribed for this offence. The Criminal Code prescribes mandatory confiscation of resources intended for financing of terrorism. A draft law amending the Criminal Code is currently in Parliament and hence the incrimination of the offence "Financing of terrorism" will be considerably extended. The new definition of offence of financing of terrorism, amended states as follows: ***"Financing of Terrorism*** **Article 449** **(***1) Anyone who in any way provides or raises money, securities, other funds or property intended entirely for financing the commission of criminal offences referred to in Articles 447, 447a, 447b, 447c, 447d and 448 of the present Code, or for financing organisations that have the aim of committing those offences, or members of those organisations,* *shall be punished to imprisonment for a term of one to ten years.* *(2) Funds referred to in Paragraph 1 of this Article shall be confiscated."*

[2] i.e. part of Recommendation 16.

	Such definition clearly states the funds intended for financing terrorist offences – money, securities, other assets or property whose purpose is for complete or partial use for financing terrorist offences, public callings to commit acts of terrorism, incitement and training to commit acts of terrorism, use of lethal device, damage and destruction of nuclear facility and endangering persons under international protection. Incrimination of the offence of “Financing of Terrorism“ will be considerably extended by adoption of the Law on Amendments to the Criminal Code, which is in the parliamentary procedure. In pursuance with the new definition of the criminal offence of financing of terrorism, this offence is done by a person who in any way provides or collects money, securities, other resources or assets intended to be fully or partially used for financing of execution of the criminal offences as under Article 447, 447a, 447b, 447c, 447d and 448 of the Criminal Code (terrorism, public invitation to execution of terrorist activities, recruiting and training for execution of terrorist activities, use of a lethal device, damage to and destruction of a nuclear facility and endangering of persons under international protection) or for financing of organisations whose aim is to execute such activities, or for financing of members of such organisations. Imprisonment for the period of one to ten years remains the prescribed punishment, along with mandatory confiscation of resources intended for financing of terrorism. In accordance with the recommendation made following the evaluation of Montenegro before the MONEYVAL Committee on 17 March 2009, the new definition will clearly specify resources intended for financing of criminal offences of terrorism - money, securities, other resources or assets intended to be fully or partially used for financing execution of criminal offences. The legal definition will be extended with the term “and other resources or assets“, in compliance with the recommendation, the Convention on the Suppression of Terrorism and the Palermo Convention. Thus, the innovated definition of the offence of “Financing of Terrorism“ also includes such activities which contribute to financing of terrorism and which are not strictly speaking collection of money and securities – therefore, provision of any resources or assets in the aim of financing of terrorism. The terms “resources“ and "assets“ shall be construed in accordance with the ratified international conventions. Furthermore, Montenegro has ratified the Convention on Prevention of Financing of Terrorism (“Official Gazette of the Federal Republic of Yugoslavia / International agreements“ 7/02), as well as Palermo, Strasbourg and Warsaw convention. Having in mind the hierarchy of normative acts stipulated by the Constitution, the terms “funds“, “properties“, “confiscations“, “seizing“, „predicate part“ and other stipulated by this convention are a constituent part of the legal order – therefore applicable in case law.
(Other) changes since the last evaluation	The innovated definition of terrorist financing offence includes activities that contribute to financing of terrorism and that are not strictly raising money and securities. This definition includes also providing funds or property for the purposes of financing of terrorism. The terms “Funds“ and “Property“ are interpreted broadly, in accordance with the ratified international conventions
Recommendation of the MONEYVAL Report	*The reference to specific criminal offences (terrorism, international terrorism and hostage taking) in Article 449 should be brought into line with the scope of the Terrorist Financing Convention and the Interpretive Note to SR II, as the scope which constitutes the criminal offence becomes narrower. Under Articles 365 and 447, only the acts, intended to cause harm (to the constitutional order of Montenegro, or the foreign state/international organisation) are criminalized, while*

	the convention requires the incrimination of any acts of violence which purpose is to intimidate a population or compel a government or international institution (to do/to abstain from doing).
Measures taken to implement the Recommendation of the Report	With amendments to the Criminal Code that are in progress, the concept of terrorism is amended and closer defined through introduction of new terrorist offences (public calling to commit acts of terrorism, incitement and training to commit acts of terrorism, use of lethal device and destruction and damaging of a nuclear facility. Terrorism offences from Article 365 and international terrorism are unified in a unique act – terrorism. Through this the citizens, the state of Montenegro, a foreign country and international organisations – and their constitutional, political, economic and social structures are protected in a unique way. Through amendments to this Article it is harmonised with the recommendations to incriminate any acts of violence whose purpose is to intimidate a population or compel a government or international institution (to do/to abstain from doing). Apart from these and incorporating new acts, any act directed against these values shall be considered financing of terrorism. The innovated definition of terrorist financing offence includes activities that contribute to financing of terrorism and that are not strictly raising money and securities.
Recommendation of the MONEYVAL Report	*The Criminal Code should be amended to incorporate the incrimination of funding of terrorist organisations and individual terrorists.*
Measures taken to implement the Recommendation of the Report	This recommendation was adopted through amendments of the Criminal Code and incrimination of the act of financing of terrorism planned and conducted both by individual terrorists and by a terrorist organisation is clearly stated. The new definition is as follows: ***"Financing of terrorism*** ***Article 449*** *(1) Anyone who in any way provides or raises money, securities, other funds or property intended entirely for financing commission of criminal offences referred to in Articles 447, 447a, 447b, 447c, 447d and 448 of the present Code, or for financing organisations that have the aim to commit those offences, or members of those organisations,* *shall be punished to imprisonment for a term of one to ten years.* *(2) Funds referred to in Paragraph 1 of this Article shall be confiscated."* It is clear that this definition includes financing terrorist organisations and individual terrorists as separate categories. Apart from that, terrorist association is also stipulated as a new criminal offence - when two or more persons associate for a longer time period in order to commit terrorist offences, endangering persons under international protection and financing of terrorism: ***"Terrorist association*** ***Article 450*** *(1) If two or more persons associate for a longer period to commit criminal acts referred to in Articles 447 to 449 of this code (terrorism offences, endangering persons under international protection and financing of terrorism),* *they shall be punished by a sentence stipulated for the act for whose commission the association was organised.* *(2) A perpetrator of an offence referred to in Paragraph 1 of this Article who prevents commission of criminal acts referred to in Paragraph 1 of this Article by*

	revealing association or in any other way, or who contributes to its revealing, *shall be punished by an imprisonment sentence of up to three years, and may also be acquitted".*
Recommendation of the MONEYVAL Report	*The solution of relating the existence of the terrorist financing offence to specific criminal offences, found under other Articles of the CC is also appropriate (IN 6). Under current legislation, terrorist financing is only considered to be a criminal offence if funds are intended for one of three specific criminal offences (Terrorism, Article 365, International Terrorism, Article 447 and Hostage Taking, Article 448). A more flexible definition which would incriminate financing. Furthermore, there needs to be an offence introduced to cover cases when funds are not linked with a specific terrorist.*
Measures taken to implement the Recommendation of the Report	Amendments to the Criminal Code introduced a completely new concept of terrorist criminal offences. Basic terrorist offence (regardless whether the act is directed against Montenegro, a foreign state or an international organisation) is stipulated in Article 447 with many forms of act of commission. This criminal offence, as well as new terrorist offences such as public calling to commit acts of terrorism (Article 447a CC), incitement and training to commit acts of terrorism (Article 447b CC), use of lethal device (Article 447c CC), destruction and damage of nuclear facility (Article 447d CC), endangering of persons under international protection (Article 448), as well as financing of terrorism (Article 449) were included and brought in line with a number of conventions aiming at prevention of acts of terrorism. In compliance with the recommendation made after the evaluation, amendments will eliminate the narrow framework within which the existence of this criminal offence is established (the present solution defines financing of three types of this criminal offence) – namely, the framework within which the existence of such criminal offence is established will be extended to all criminal offences in the area of terrorism, whose scope will be widened by amendments to the law. Thus, the framework for existence of this offence will not include only criminal offences of terrorism, international terrorism and taking of hostages; in addition to these offences, it will also include public invitation to execution of terrorist activities, recruiting and training for execution of terrorist activities, use of a lethal device, damage to and destruction of a nuclear facility and endangering of persons under international protection. In this way the deficiencies of the definition which has been assessed as narrow are eliminated and a more flexible and clearer definition of this offence is created. Apart from adding new articles as afore mentioned, the criminal offence of hostage taking was changed and is as follows: ***"Endangering persons under international protection*** ***Article 448*** *(1) Anyone who conducts abduction or some other act of violence upon a person under international legal protection,* *shall be punished by an imprisonment sentence of two to twelve years.* *(2) Anyone who violates official premises, a private apartment or a means of transport of a person under international legal protection, in the manner that endangers his/her security and personal freedom,* *shall be punished by an imprisonment sentence of one to eight years.* *(3) If an act referred to in Paragraphs 1 and 2 of this Article results in death of one or more persons, the offender shall be punished by an imprisonment sentence of five to fifteen years.* *(4) If in commission of an act referred to in Paragraphs 1 and 2 of this article, the*

	offender committed a premeditated murder of a person, *he/she shall be punished by an imprisonment sentence of minimum ten years or an imprisonment sentence of fourteen years* *(5) Anyone who endangers security of persons referred to in Paragraph 1 of this Article by a serious threat to attack him/her, his/her official premises, private apartment or a means of transport, shall be punished by an imprisonment sentence of six months to five years."*
Recommendation of the MONEYVAL Report	*Article 449 of the Criminal Code should be brought into line with international standards.*
Measures taken to implement the Recommendation of the Report	In accordance with the recommendations, apart from the changes of the Article itself relating to financing of terrorism, the Law on Amendments of the Criminal Code introduces a new article – terrorist association. This act stipulates as a criminal offence the association of two or more persons for a longer time period in order to commit acts of terrorism. Article 449 of the Criminal Code, as it is stated in the proposal of the Amendments of Criminal Code, is in compliance with the international standards. Indeed, in accordance with the recommendation made after the evaluation, the definition of this criminal offence, namely financing of terrorism, has been improved also in terms of defining in a clearer manner financing of both individual terrorists and terrorist organisations. This has eliminated the perceived deficiency in the current definition, namely it does not make clear difference between financing of an individual terrorist and financing of a terrorist organisation. Additionally, through adoption of amendments, the Criminal Code will define another criminal offence – terrorist association – when two or more persons associate for a longer period of time in order to execute criminal offences in the area of terrorism. In accordance with the recommendation stating that this Article (449) of the Criminal Code should be harmonised with international standards, from the viewpoint of everything mentioned above, we deem that all the perceived deficiencies have been defined, that all the recommendations have been accepted and incorporated in the planned amendments, and that the new definition of this criminal offence, after the Law on Amendments to the Criminal Code has been adopted, which is currently in the parliamentary procedure, will be even more efficient and provide better quality concerning its implementation in practice.
(Other) changes since the last evaluation	

Special Recommendation IV (Suspicious transaction reporting) **I. Regarding Financial Institutions**	
Rating: LC	
Recommendation of the MONEYVAL Report	
Measures taken to implement the Recommendation of the Report	

(Other) changes since the last evaluation	

Special Recommendation IV (Suspicious transaction reporting) II. Regarding DNFBP	
Recommendation of the MONEYVAL Report	
Measures taken to implement the Recommendation of the Report	
(Other) changes since the last evaluation	

3. *Other Recommendations*

In the last report the following FATF recommendations were rated as "partially compliant" (PC) or "non compliant" (NC) (see also Appendix 1). Please, specify for each one what measures, if any, have been taken to improve the situation and implement the suggestions for improvements contained in the evaluation report.

Recommendation 6 (Politically exposed persons),	
Rating: PC	
Recommendation of the MONEYVAL Report	*The lack of awareness as regards PEPS and the consequent lack of proper procedures to address the risk should be addressed through proper training to be followed by the establishment of adequate procedures to address this risk.*
Measures taken to implement the Recommendation of the Report	In its internal acts on risk analysis, a bank is obliged to assess and consider client risk, including clients who are politically exposed persons pursuant to the rules defined in the Draft Guidelines on bank risk analysis aimed at preventing money laundering and terrorism financing, chapter 2 section 1.2.5.1.2, prescribing the following: "Procedure of persons to be listed as politically exposed persons Pursuant to the provisions of the LPMLTF, a politically exposed person is `a natural person that is acting or has been acting in the last year on a distinguished public position in a state, including his/her immediate family members and close associates` (Article 27). In order to determine the politically exposed persons and his/her immediate family members and close associates within the meaning of the LPMLTF, a bank may act in one of the following manners: • offer a client to fill in a form (enclosed to these Guidelines and making an integral part hereof, the Form PEP); • obtain the information from public available sources; • obtain the information based on the review of databases covering the lists of

politically exposed persons (World Check PEP List, internet inquiry, etc).
The procedure of identifying close associates to politically exposed persons is applied if a bank estimates that such a relationship exists, based on the indisputable facts.
A bank is obliged to perform client identification in line with the LPMLTF and the procedure shall include one of the manners for determining politically exposed persons as specified under paragraph 2 of this section.
Upon determining that the client is a politically exposed person, the employee of the bank shall perform the enhanced customer verification (Article 25 of the LPMLTF) that shall cover additional measures in the following cases:

- entering into business relationship or executing transaction from Article 9 paragraph 1 item 2 of this Law (one or more transactions of or exceeding EUR 15,000),
- when it estimates, due to the nature of the business relationship, the client's business profile and/or other circumstances connected with the client, that there is or could exist the risk of money laundering or terrorism financing.

In addition, as a part of the enhanced client verification – the politically exposed person – in line with the LPMLTF, the employee of the bank shall:
• obtain a written consent from the responsible person in the bank before the establishing of a business relationship with such a client;
• acquire information on the source of funds and property which are the subject of the business relationship and/or transaction, from personal and other identification documents submitted by the client; if the specified information is not possible to obtain from the submitted documents, the required information shall be acquired directly from the client's written statement;
• after the establishment of the business relationship, closely monitor transactions and other business activities of the politically exposed person with the bank, particularly considering the purpose of the transaction, as well as comparing it with his/her standard business operations.

Additional measures to be taken by bank within the enhanced client verification procedure				
Case prescribed in the Law ↓	1) Consent from the responsible person in the bank ↓	2) Acquiring additional documents and information ↓	3) Additional examination and monitoring of the client's business operations ↓	4) Additional measures ↓
Politically exposed person	Yes	Set of data defined under Art. 27 of LPMLTF	Yes	As estimated by the bank

A bank is obliged to determine the list of politically exposed persons which shall be available to the employees of the bank in direct contact with clients.
<u>Procedure of cancellation of obligation of treating persons as politically exposed persons</u>

	A bank shall, by way of internal act, prescribe the procedure of cancellation of obligation of treating a client as politically exposed person. This implies the obligation on the bank to exclude a person from the list of politically exposed persons, as well as members of his/her immediate family and close associates, one year following the termination of activity of the politically exposed person at a prominent position in a country. After the establishment of a business relationship with the politically exposed person, members of his/her family and close associates in accordance with the LPMLTF, the bank shall keep separate records on these persons and transactions. The bank is obliged to regularly update its list of politically exposed persons in order to conduct customer due diligence in line with the LPMLTF for those clients who were not politically exposed persons within the meaning of the LPMLTF at the time of establishing the business relationship with the bank.“ On 8th February 2010, at the Bank Association of Montenegro, representatives of the Central Bank of Montenegro held the meeting with the Committee for the prevention of money laundering and terrorism financing, where they discussed the draft Guidelines on Developing Risk Analysis with a view to Preventing of Money Laundering and Terrorist Financing for Banks. Also, in this meeting, detailed explanations were given, to the representatives of the banks, related to the identification of PEPs, with special emphasis on the form and content of the Questionnaire for identifying politically exposed persons. After adopting the Guidelines on developing risk analysis with a view to preventing money laundering and terrorist financing the APMLTF, in co-operation with OSCE, organised a two-day workshop for compliance officers, on 3rd and 4th November 2009, in Podgorica. The subject of the workshop was “Preventing money laundering and terrorist financing in financial and non-financial sector. The participants were employees from different commercial banks, participants at the capital market, car dealers, leasing companies, casinos. The Guidelines on risk analysis were presented at this workshop. The Guidelines for developing risk analysis, determined by the APMLTF, together with the Questionnaire for Identifying PEPs were presented at the Workshop. The Securities and Exchange Commission prescribed specific procedures to be followed in case of PEPs and these are very precisely defined in the article 12 of the Instruction of the Securities and Exchange Commission. Obliged entities are obliged to determine if the client is politically exposed person in accordance with the article 12 of the Instruction of the Securities and Exchange Commission of on risk analysis of money laundering, „know your client” procedures and other procedures for recognising suspicious transactions of November 28, 2008. To determine politically exposed persons and members of their close family and close associates by Law, Capital market participants may act on some of the following ways: a) By filing the written form by the customer; b) Collecting information from public sources; c) Collecting information based on insight on data bases that includes the lists of politically exposed persons (*World Check PEP List*, etc). d) Procedure of determining close associate of politically exposed persons is followed if the relationship with associate is publicly known or if capital market participant has reason to think that relationship exists. Therefore, during determining the persons who are considered as a close associates of politically exposed persons,

	capital market participants are not expected to take active researching about this. Before establishing business relationship with politically exposed person, participant of securities market is obliged to: – Collect data about founding sources and property which are object of business relationship, transactions, from personal and another identification of customer, and if it is not possible to obtain such a data from the statements submitted, there are collected directly from written statement of the client; – Obtain written approval of responsible person according to internal acts of the participant before establishing business relationship with customer. Approval of responsible person has to be given in written, in printed or in electronic form. After establishing business relationship with politically exposed person, members of his close family and close associates by Law, Capital market participants is obliged to keep records about this persons and transactions which are taken on behalf and for the account of those persons. After obtaining the approval from authorised person there is no need for approval of executing each transaction on behalf and for the account of the client, but capital market participant is obliged to follow transaction with special attention and other business activities by a politically exposed person within organisation and, if needed, notify authorised person in the shortest possible deadline about those transactions. It is considered that a need determined in the Article 6 exists if transaction is not adjusted to the sources of funds on client's account. The capital market participant are obliged to ordinarily update their lists of politically exposed persons in order to implement procedures of enhanced customer verification according to Law for the client who, in time of establishing business relationship were not politically exposed persons according to Law. The capital market participants are obliged to keep the data about politically exposed persons in electronic form. The form for PEPs is prescribed by the Guidelines on risk analysis with the view to prevent money laundering and terrorist financing, and the Guidelines are forwarded to all operators of the games of chance on the territory of Montenegro and also in informal communication certain instructions were given to all operators of the games of chance. By its risk analysis Guidelines concerning prevention of money laundering and terrorist financing, ISA will also cover PEPs issue, and will prescribe a Form intended for the insurance companies especially regarding this issue. According to the competence of the APMLTF from the Article 64, item 5 to prepare and issue recommendations or guidelines for uniform implementation of the Law on AML/CTF, in July 2009 representatives of APMLTF participated at one- day workshop organised for employees from one commercial bank and its subsidiaries (14 participants). At this workshop representatives of APMLTF have pointed out the significance of implementation of legal provisions related to PEPs. Additionally, APMLTF employees, in their daily communication with compliance officers, through providing professional opinion and interpretation of the provisions of the Law, specify the necessity of applying legal provisions referring to PEPs. Within IPA 2007 Twinning project "Fight against organised crime and corruption" experts form United Kingdom and Northern Ireland, in co-operation with APMLTF, during May 2009 organised trainings for officers having a direct communication with customers. The training was conducted at 9 commercial banks with 100

	participants. At the beginning of September 2009, trainings for supervisory bodies under the Law on the Prevention of Money Laundering and Terrorist Financing were held for the following supervisors: APMLTF, Ministry of Finance, Insurance Supervision Agency, Department of Public Revenues, Central Bank, Administration for Games on Chance, Securities Commission. The workshop on Inter-agency co-operation in relation to organised crime and corruption was held in the period from 7th to 11th September 2009. The participants at this workshop were representatives from: APMLTF, Police Directorate, Directorate for Anticorruption Initiative and Ministry of Internal Affairs and Public Administration. After the Report of the MONEYVAL Committee has been adopted the employees of the Police Directorate accepted the recommendations given in the Report. Due to that there were organised 4 seminars on the prevention of money laundering and terrorist financing as well as financial investigations. The mentioned seminars were organised at the Police Academy in Danilovgrad and 45 officers involved in PML/TF participated at these seminars that were organised by APMLTF or international organisations. At these joint seminars together with officers from APMLTF and State Prosecutor's Office, participants were mainly higher level officers that have, made reports on the content of the seminars, and in such manner informed the heads of their sectors and field officers. Also, after the adoption of the Report of the MONEYVAL Committee, Police Academy introduced as regular subject „Money laundering and Corruption" and through this subject students quire the first and the most significant knowledge on this type of criminal activity. With a view to training its employees the Customs Administration signed an agreement with Faculty of Law Podgorica.

Recommendation 8 (New technologies and non face-to-face business)	
Rating: PC	
Recommendation of the MONEYVAL Report	*A requirement for financial institutions to have policies and procedures to address the risk of misuse of technological developments in ML/TF schemes should be introduced.*
Measures taken to implement the Recommendation of the Report	In their polices and procedures, banks have already prescribed certain rules regarding the protection from misuse of new technologies for the purposes of money laundering and terrorism financing, and now they are obliged to harmonise their policies and procedures with the rules and standards contained in the Central Bank's Guidelines on bank risk analysis aimed at preventing money laundering and terrorism financing, chapter 3 paragraph 4 that reads: "With a view to ensuring a proper risk management in the area of preventing money laundering and terrorism financing, a bank shall reduce its exposure to risk arising from new technologies providing anonymity (electronic or internet banking, electronic money, etc.), i.e. the bank is obliged to define in its policies and procedures in particular, but not limited to, the following: • identification of parties using electronic banking services; • authenticity of the signed electronic document; • reliable measures against the forgery of documents and signatures; • systems ensuring and enabling safe electronic banking; • other requirements in accordance with positive regulations governing the aforesaid business area." This requirement for securities providers is imposed by the newly adopted Rules on

	Conduct of Business of Licensed Market Participants that are published in the Official Gazette of Montenegro ("Official Gazette of Montenegro", No. 78/09 and 87/09). The Securities and Exchange Commission implemented this recommendation by the article 22 par.6-9 of the Rules on Conduct of Business of Licensed Market Participants that are published in the Official Gazette of Montenegro ("Official Gazette of Montenegro", No. 78/09 and 87/09). These Rules specifically regulate the procedures to be followed by the licensed market participants if the client uses electronic means of communication to submit an order or conclude a contract. "Client, who gives orders by phone, fax or electronically, may give the same with authorisation by identity code which licensee shall assign to a client when signing a contract. A client is obliged to keep his/her identity code as a secret, and may not make it available to third persons. Licensee is obliged to check client's identity through identity code, contained in any contract prescribing possibility of submitting orders by phone, fax or electronically or in any other manner which does not imply client's face to face transaction. When prescribing possibility of electronic submitting of client's orders, licensee is obliged to provide: - reliable manner of client identification; - that all necessary elements of an order are stated in the electronic message; - a record of exact time when the order arrived to an e-mail and time of its entry in the order book; - sending of reply to a received order, where the original message of order sender is clearly visible; When prescribing possibility of electronic submitting of client's orders, licensee shall retain the right to refuse order execution, if the order is unclear and/or ambiguous, and he/she shall inform a client on that in the same way it accepted an order."
(Other) changes since the last evaluation	Rules on Conduct of Business of Licensed Market Participants that are published in the Official Gazette of Montenegro ("Official Gazette of Montenegro", No. 78/09 and 87/09)
Recommendation of the MONEYVAL Report	*Regulations should clearly establish the obligation to obtain information on the purpose and intended nature of the business relationship for non-face to face business.*
Measures taken to implement the Recommendation of the Report	Chapter 3 paragraph 6 of the Guidelines on bank risk analysis aimed at preventing money laundering and terrorism financing reads: "Banks must have such policies and procedures to prescribe the requesting of all information on the purpose and the nature of business relationships or transactions with clients who are not present in person and they are obliged to apply these policies and procedures when establishing a business relationship with a client and in conducting the customer due diligence." The obligation of the licensed market participant to obtain information on the purpose and intended nature of the business relationship is imposed by the article 5 par. 5 and article 11 par. 2 of the Rules. The article 5 par. 5 of the Rules prescribe: "Licensee shall not give advice related to securities business, nor realise transactions for the client's account, until he/she determines that he/she possesses all facts revealed to him/her by his/her client and other relevant facts about client he/she is aware of or he /she should have knowledge about."

	The article 11 par. 2 of the Rules prescribe: "In order to provide that client understands actual risk, licensee is obliged to: - familiarize with client's financial status, his/her investment experience and other circumstances related to client, in order to provide him /her with appropriate service; put at client's disposal all necessary information (including information on risks) in order that client can make appropriate investment decisions."
(Other) changes since the last evaluation	

Recommendation 11 (Unusual transactions)	
Rating: NC	
Recommendation of the MONEYVAL Report	*Financial institutions should be required to examine as far as possible the background and purpose of unusual transactions. Enforceable requirements to set forth the finding of such examinations in writing should equally be provided. In addition specific enforceable requirement should be put in place for financial institutions to keep such findings available for authorities and auditors for at least five years.*
Measures taken to implement the Recommendation of the Report	Rulebook on Indicators for recognising suspicious clients and transactions ("Official Gazette of Montenegro ", No. 69/09, from 16th October 2009) adopted by Ministry of Finance and due to that the following List of indicators for recognising suspicious clients and transactions was established : - List of Indicators for banks, - List of Indicators for capital market, - List of Indicators for the Customs Administration, - List of Indicators for the Department of Public Revenues, - List of Indicators for leasing companies, - List of Indicators for auditors, - List of Indicators for accountants, - List of Indicators for lawyers and - General indicators. In the group of indicators referring to unusual changes on the account, indicator no.47 „Transactions that are recognised as unusual by employees with the bank, in accordance with their experience and knowledge.“ these transactions are treated as suspicious transactions. Also, in the group of suspicious transactions indicators with banks there is indicator no.9 stating „Client executes transactions which are unusual for him/her.“ Similar indicators are in the group for auditors (indicator No 6 and 8)
(Other) changes since the last evaluation	

Recommendation 16 (Suspicious transaction reporting) Regarding DNFBP	
Rating: NC	
Recommendation of the MONEYVAL Report	*A prohibition against tipping off should be made specifically applicable to lawyers.*
Measures taken to	Article 80 of the LPMLTF defines that reporting entities and employees with

implement the Recommendation of the Report	reporting entities, members of governing, supervising or managing bodies, or other persons, to which data from Article 71 of this Law were available, may not reveal to a customer or third person: 1. that data, information or documentation on the customer or the transaction, from Article 33 paragraph 2, 3 and 4, Article 43 paragraph 1*, Article 48 paragraph 1, 2 and 3, Article 49 paragraph 1 and 2* of this Law, are forwarded to the competent administration body ; 2. that the competent administration body on the basis of Article 51 of this Law, temporarily suspended transaction or in accordance with that gave instructions to the reporting entity; 3. that the competent administration body on the basis of Article 53 of this Law demanded regular supervision of customer's financial business; 4. that against customer or third party is initiated or should be initiated investigation for the suspicion of money laundering or terrorist financing . The information about the facts from paragraph 1 of this Article and notification on suspicious transactions or information about other offences from Articles 55 and 56 of this Law, are the official secret and designated as such, in accordance with Law. On removing the official secret designation, from paragraph 2 of this Article shall decide the authorised person of the Administration. Prohibition of giving information from paragraph 1 of this Article may not be applied on: 1. data, information and documentation, that are, in accordance with this Law obtained and kept by reporting entity, and necessary for establishing facts in criminal proceedings, and if submitting those data in written form is required or ordered by the Competent court, and 2. data from item 1 of this Article, if it is demanded by supervision body from Article 86 of this Law for the reasons of carrying out the provisions of this Law and regulations passed on the basis of this Law. *applicable to lawyers
(Other) changes since the last evaluation	
Recommendation of the MONEYVAL Report	*More targeted training to sectors that pose the greatest risk should be considered.*
Measures taken to implement the Recommendation of the Report	Representatives of all categories of reporting entities participate at the training courses that APMLTF organises for compliance officers and employees with the reporting entities which have a direct contact with customers.
(Other) changes since the last evaluation	

Recommendation 21 (Special attention for higher risk countries)	
Rating: NC	
Recommendation of the MONEYVAL Report	*Financial institutions should be required to give special attention to business relationships and transactions with persons from or in countries which do not or insufficiently apply the FATF recommendations. Effective measures should be put in place to ensure that financial institutions are advised of concerns about weaknesses*

	in the AML/CFT systems of other countries and consideration should be given to the development of appropriate countermeasures as set out in the essential criteria to Recommendation 21.
Measures taken to implement the Recommendation of the Report	**Chapter 2 section 1.1 paragraph 4** of the Draft Guidelines on bank risk analysis aimed at preventing money laundering and terrorism financing reads: "In its internal act, a bank shall define conditions for refusing the establishment of a business relationship with a client, and in particular: • If the home country of the client or the beneficial owner of the client is on the list of non-cooperative countries published by the Financial Action Task Force – FATF, the list of offshore jurisdictions, or the list of countries deemed risky by the authority based on its own assessment; • If the client or the beneficial owner of the client comes from the country which has been subject to measures in line with the UN Security Council resolutions; • If the client is on the list compiled in line with the UN Security Council resolutions; " **Chapter 2 section 1.3.1** of the Draft Guidelines on bank risk analysis aimed at preventing money laundering and terrorism financing reads: **"Risk factors used for establishing the risk of an individual client or a group of clients and the business relationship** Internationally accepted standards used as the basis for preparing risk analysis with a view to preventing money laundering and terrorism financing (e.g. FATF recommendations and Wolfsberg guidelines) shall cover the following risk factors: **- <u>Client risk factors</u>:** risk factors relating to the client's status or activity (e.g. state authority, a politically exposed person, a client whose activity is connected with cash transactions, non-profitable organisations, and the like). **- <u>Risk factors connected with business relationship</u>**: risk of business relationship, for example, with a client whose home country does not follow the standards in the prevention of money laundering and terrorism financing, with a politically exposed person, and other business relationship deemed by the bank to involve high risk. **- <u>Risk factors connected with geographical region</u>**: countries having in place inadequate systems for the prevention of money laundering and terrorism financing, countries with high levels of corruption or criminal activities, countries subject to restrictive measures of international organisations; Risk factors for determining the risk of an individual client or a group of clients, the business relationship, and risk factors connected with the geographical region are illustrated in the risk matrix. In addition to risks presented in the risk matrix, a bank may define additional factors in relation with the specific nature of the client1`s business." The obligation of providing special attention to business relationships with the clients where AML/CFT procedures are not implemented is imposed by the Securities and Exchange Commission Instruction. This Instruction in the Article 2 items *a* and *b* prescribes: "Participants at the capital market are obliged to establish risks factors upon which shall determine acceptability of the clients, especially based at the following facts: a) Home country of the client, home country of the majority founder, and/or real owner of the client regardless of the position of such country on the list of non-cooperative countries and territories issued by the international body for control and combating of money laundering, on a list of countries presented as off-shore zones or uncooperative jurisdiction or on list states which participant on securities market considers risky upon its own estimations.

	b) Home country of the person who conducts transactions with the client, regardless of the position of such a country at the lists from the item a) above; And article 3 paragraph 1 prescribes: "Capital market participants establish acceptability of the client depending on a risk factors from the article 2 of this Instruction and may refuse to conclude a contract with the customer in relation to whom some of the abovementioned risk factors are established, or concluding or terminating of the already concluded contract condition upon fulfilment of some specific requirements prescribed by the general act of the capital market participant".
(Other) changes since the last evaluation	

Recommendation 24 (DNFBP – Regulation, supervision and monitoring)	
Rating: PC	
Recommendation of the MONEYVAL Report	*A comprehensive register of all reporting entities should be developed by APMLTF.*
Measures taken to implement the Recommendation of the Report	Out of all categories of reporting entities, subject to inspection control performed by Reporting Entities Control Department of the APMLTF, the real estate area is the most controlled one and there are comprehensive records. Also, this area is closely connected with the construction business. Companies that deal with construction business, besides its main business activity, they also deal with real estate trade even if they are not registered for it . In relation to NGOs there is a comprehensive register that includes 4000 NGOs. Most of registered NGOs are not active or they do not have any registered transaction which could be defined, on any basis, as suspicious. The number of other reporting entities categories supervised by APMLTF is lower than the number of previously described categories of reporting entities.
Recommendation of the MONEYVAL Report	*Guidelines to assist DNFBPs in implementing and complying with respective AML/CFT requirements are, at should be developed. Adequate and appropriate feedback on suspicious transaction reporting for DNFBPs should be provided.*
Measures taken to implement the Recommendation of the Report	The APMLTF provide information, in written form, to the reporting entity or other requester, on obtaining and analysing data, information and documentation related to persons or transactions for which there are reasonable grounds for suspicion in criminal offence of money laundering or terrorist financing. The APML will not provide the mentioned information if it is assessed that such informing could have harmful effects for the process and outcome of the procedure, as it is defined in Article 57 of the LPMLTF.
(Other) changes since the last evaluation	

Recommendation 32 (Statistics)	
Rating: PC	
Recommendation of the MONEYVAL	*Clear comprehensive and well-structured statistics should be kept systematically. Such statistics should differentiate the amounts of assets, types of measures, duration of measures and primarily request/imposition ratio, etc.. These statistics*

Report	*should then be utilised to measure the effectiveness of the system of confiscation, freezing and seizing of proceeds of crime..*
Measures taken to implement the Recommendation of the Report	Besides the statistical tables provided in this Report, the APMLTF is keeping statistics on inspection control, comprehensive statistics on misdemeanour procedure and statistics related to exchanging information with foreign FIUs *Department of Public Revenues possesses appropriate software and data base that enables collecting, analysing and forwarding data. This data base is upgraded continuously and upon appropriate requests is available to all authorities involved in the system of prevention of money laundering and terrorist financing* . The Project of Integrated registration and payment is in the final phase and more efficient data access and keeping statistics will be provided by this project. **Note:** The Central Bank of Montenegro has presented the statistical tables in the Chapter 4 – Statistics hereof Supreme State Prosecutor's Office keeps comprehensive statistics for all criminal offences and for the criminal offence of money laundering. In the attachment you can find table in which is presented the number of criminal offences money laundering in the period of 2004 until December 31st 2009, the way the cases are solved, the number of the temporary measures suggested, amount of the proceeds of crime, suggested confiscation and the number of the convictions. This kind of statistical data gives the possibility to measure the efficiency Department of Public Revenues possesses appropriate software and data base that enables collecting, analysing and forwarding data. This data base is upgraded continuously and upon appropriate requests is available to all authorities involved in the system of prevention of money laundering and terrorist financing . The Project of Integrated registration and payment is in the final phase and more efficient data access and keeping statistics will be provided by this project
(Other) changes since the last evaluation	

Recommendation 33 (Legal persons – beneficial owners)	
Rating: PC	
Recommendation of the MONEYVAL Report	*The acquisition of information on beneficial owners by the agencies and institutions which deal with clients form abroad seems to be less effective. Considering the very intensive involvement of foreign legal entities on the Montenegrin real-estate market and rather poor information on beneficial ownership in such entities, this might present a considerable risk of abuse of such legal entities for money laundering and terrorist financing and it is recommended that financial institutions and DNFBPs be reminded to apply the same standards to overseas customers as to domestic.*
Measures taken to implement the Recommendation of the Report	As a part of verification and examination of the client being a legal person, in addition to identification, a bank is obliged to identify the actual owner of such a legal person. In line with provisions of the LPMLTF, a bank shall apply the measures required for acquiring information on the person being the actual owner. In case of a high-risk client, a bank must confirm the acquired information if it is not received from a reliable and independent source (e.g. if a written statement of a legal representative was the only source of information for determining the client's identity, a bank must check the information to the extent that will enable it to understand the ownership of the legal person and its controlling structure, in order to identify all beneficial owners of the client).

	Beneficial owner of a legal person within the meaning of Article 19 of the LPMLTF is considered: (1) a natural person who indirectly or directly owns more than 25% of the shares, voting rights and other rights, on the basis of which he/she participates in the management, or owns more than a 25% share of the capital or has a dominating influence in the assets management of the business organisation, and (2) a natural person that indirectly ensures or is ensuring funds to a business organisation and on that basis has the right to influence significantly the decision making process of the managing body of the business organisation when decisions concerning financing and business are made. As per the aforesaid definition, a beneficial owner is a natural person participating (directly or indirectly) in the legal person's management based on 25% of share. When identifying the beneficial owner, it is necessary to identify the natural person's ownership share in that legal person, as well as the ownership share of a legal person controlled by the same natural person. A bank may obtain ownership information based on the original or a certified copy of excerpt from the court registry or any other official registry submitted by the legal representative or the person authorised on behalf of the legal person. In addition, a bank may apply provisions of the LPMLTF enabling the obtaining of information on the beneficial owner through a direct inquiry into the court registry or any other public registry or through other available sources. If all the prescribed information regarding the beneficial owner (e.g. date and place of birth) cannot be obtained from the court registry or any other official registry, a bank may obtain the lacking information from the legal representative or the authorised person. A beneficial owner of an institution or other foreign legal person (trust, fund and the like) that receives, manages or allocates assets for certain purposes, in the context of this Law, shall be considered: (1) a natural person, that indirectly or directly controls more than 25% of a legal person's asset or of a similar foreign legal entity (2) a natural person, determined or determinable as a beneficiary of more than 25% of the income from property that he/she manages. A bank must confirm the ownership structure of clients - legal persons and acquire all necessary information on their beneficial owners, in accordance with the LPMLTF. If the registered office of the legal person is in Montenegro, the bank is recommended to perform direct inquiry into the court registry or any other public registry in order to obtain or confirm information on the beneficial owner of such a legal person. If one of the beneficial owners is a foreign legal person, the bank is recommended to acquire the information on the beneficial owner of such a legal person based on the original or a certified copy from a foreign registry or from business documents to be

	submitted by the legal representative or the authorised person on behalf of the client. Since the bank has no information regarding the authenticity of information from other countries, it is recommended that the legal representative or the authorised person of the client submit an electronic statement from the public registry in the foreign country. If the legal representative, due to objective reasons, cannot provide the requested documentation that clearly shows the information on the beneficial owner, such information shall be obtained from the written statement to be submitted by the legal representative or the authorised person of the client. A bank shall also request a written statement from the legal representative in case of any suspicion regarding the accuracy of the submitted information. If the legal representative does not show his/her willingness to cooperate with the bank in offering the requested information and thus rendering the identification of the beneficial ownership impossible, the bank should not establish the business relationship with the client. Also, in case the client avoids to submit the legally requested information, a bank is recommended to use this as the indicator for detecting suspicious activities of the client involving money laundering and terrorism financing. A bank must adopt the procedures for identifying beneficial owners, taking into account the aforesaid recommendations and/or instructions. If a bank is still unable to acquire information on the beneficial owner in spite of the undertaken actions (even after a detailed analysis of the ownership structure), due to the complexity of the structure itself, a bank shall be allowed to establish or continue such a business relationship, provided that it classifies the client as a high-risk client, which requires enhanced monitoring of business activities. It should be underlined that this applies to cross-border cases and it does not represent normal practice. The aforesaid deviation does not mean that procedures for identifying the beneficial owner should be excluded - in such cases a bank has to prove to the competent authority that it has properly applied the procedure for identifying the beneficial owner and that that is a special case of complex ownership which justifies the bank's action. The bank is also recommended to deem such a complex ownership structure as a potential reason for reporting suspicious transactions." In addition, in their internal acts (policies and procedures), banks have already prescribed the procedure for identifying beneficial owners, both natural and legal persons, which implies the use of information from the relevant public registries. Clients are also obliged to inform the bank in writing on any changes in their beneficial owners.
Recommendation of the MONEYVAL Report	*Consideration should be given to the risk of foreign bearer shares being sold in Montenegro.*
Measures taken to implement the Recommendation of the Report	The bearer shares in Montenegro may not be issued. The Law on Securities ("Official Gazette of Montenegro", No. 59/00 and 28/06). Article 5 of the Law on Securities prescribe:

	"*Securities issued in accordance with this Law must be registered at the Central Depository Agency that is established and operates in accordance with this Law.* *The rights and obligations related to the securities shall start upon registration at the Central Depository Agency*." Article 100 par. 1 and 2 of the Law on Securities prescribes: "*The owner of the account in the Central Depository Agency in which the security is recorded shall be considered the owner of the dematerialized security.* *The Central Depository Agency statement is the only legal proof of ownership of securities*." Foreign bearer shares may not be traded at the stock exchanges in Montenegro. Article 26 of the Law on Securities prescribes: "*No shares shall be traded on a licensed security market other than shares issued by a registered issuer.*"
(Other) changes since the last evaluation	

Special Recommendation I (Implement UN instruments)	
Rating: PC	
Recommendation of the MONEYVAL Report	*The incrimination of money laundering is limited to actions, defined as "business operations", which is narrower than the convention and this formulation should be further refined.*
Measures taken to implement the Recommendation of the Report	As explained in detail in the explanation of the measures taken according to recommendations of MONEYVAL relating to Recommendation 1 FATF (money laundering offence), this shortcoming was removed by the Law on Amendments to the Criminal Code, which is in the adoption procedure. **Please see the answers in the Recommendation 1 (money laundering offence).**
Recommendation of the MONEYVAL Report	*Laws and mechanisms for immediate freezing of the funds belonging to or intended for the designated terrorist organisations or individuals as defined by Resolution S/RES/1267 (1999) should be put in place.*
Measures taken to implement the Recommendation of the Report	Based on the Article 9 of the Constitution of Montenegro on the grounds of which the confirmed and published international contracts as well as commonly accepted regulations of international law which make constituent part of domestic legal order, as well as the fact that the UN Charter, bearing in mind that Montenegro is an UN member, represents international agreement Montenegro accepted (Independence Decision: UN Charter published in the Official Gazette of RFY 69/45), Montenegro is under obligation to implement measures adopted on the grounds of the Chapter VII of the UN Charter. In accordance with the EU National Integration Program for Montenegro the passing of the Law was planned for the end of 2011. in order to prepare for application and enactment of restrictive measures, jurisdictions of specific state institutions, as well as keeping records on natural and legal persons against which international restrictive measures have been introduced, and/or create legal framework for introduction of unilateral restrictive measures., Ministry of Foreign Affairs initiated the procedure of collecting all relevant international documents, EU regulations, as well as the guidelines related to implementation of all restrictive measures categories. Also, in order to determine the mechanism for overall

	regulation of the given area comparative analyses of the legal solutions of the states in the region are performed. The models of the established entities whose jurisdiction is to update the list are considered, as well as the relation of the laws on restrictive measures with other legal documents dealing with the issue of sanctions introduction. At this stage the model of introducing the institute of,, freezing assets'' (in a manner S/RES/1267) into the legal system of Montenegro, and/or whether it is more relevant to make it a part of criminal legislation or introduce it with the Law on restrictive measures.
(Other) changes since the last evaluation	

Special Recommendation III (Freeze and confiscate terrorist assets)	
Rating: NC	
Recommendation of the MONEYVAL Report	*A central authority at national level to examine, integrate and update the received lists of persons and entities suspected to be linked to international terrorism before sending them to the financial sector and DNFBP should be introduced.*
Measures taken to implement the Recommendation of the Report	After reviewing the Report of the MONEYVAL Committee on the third round of detailed assessment of 17th March 2009, with the conclusion of the Government of Montenegro of 23rd April 2009, the Ministry of Foreign Affairs, the Ministry of Justice, the Ministry of Internal Affairs and Public Administration and the Administration for Prevention of Money Laundering and Financing of Terrorism were put in charge to consider the method of application of the Special Resolutions of the United Nations Security Council S/RES/1267 (1999), S/RES/1373 (2001) and S/RES/1452(2002) and propose to the Government the measures for their implementation Although there is still no legal framework defining the system of publishing, or informing, integrating and updating the received lists of persons and companies suspected to be related to international terrorism, there is a practice to, after receiving such lists from the Permanent Mission at the United Nations Headquarters in New York, the Ministry of Foreign Affairs forwards the lists to the Ministry of Finance and Police Directorate. APMLTF receives, through its Department for National and International Co-operation, MONEYVAL and FATF statements referring to non cooperative countries with significant risk of money laundering and terrorist financing. After processing, the statements are forwarded to Analytics Department which, in written form, notifies all reporting entities under the Law on the Prevention of Money Laundering and Terrorist Financing. The statements are also published on the APMLTF website.
Recommendation of the MONEYVAL Report	*A domestic mechanism to enact S/RES/1373 (2001) should be implemented to be able to designate terrorists at national level as well as to give effect to designations and requests for freezing assets from other countries.*
Measures taken to implement the Recommendation of the Report	This issue is planned to be regulated by the Law on restrictive measures.

Recommendation of the MONEYVAL Report	*Procedures for evaluating de-listing requests, for releasing funds or other assets of persons or entities erroneously subject to the freezing and for authorising resources pursuant to S/RES/1452 (2002) should be adopted.*
Measures taken to implement the Recommendation of the Report	This issue is planned to be regulated by the Law on restrictive measures
Recommendation of the MONEYVAL Report	*Practical guidance to the financial institutions and DNFBP concerning their responsibilities under the freezing regime as well as for the reporting of suspicious transactions that may be linked to terrorism financing should be issued by the authorities.*
Measures taken to implement the Recommendation of the Report	The Guidelines on Developing Risk Analysis with a view to Preventing Money Laundering and Terrorist Financing define: The customers that present high risk from money laundering and terrorist financing are included in customers with the permanent residence or registered office: 1. in the state that is non EU member state or did not sign EU pre accession agreement, 2. in the state that is, based on assessment of the competent international organisations, known for production or well organised drug trafficking (Middle and Far East countries known for heroin production: Turkey, Afghanistan, Pakistan and golden triangle countries (Myanmar, Laos, Thailand), South American Countries known for cocaine production Peru, Columbia and neighbour countries, Middle and Far East Countries, Central American Countries known for Indian hemp production: Turkey, Lebanon, Afghanistan, Pakistan, Morocco, Tunis, Nigeria and neighbour countries, Mexico), 3. state that is, based on the assessment of the competent international organisations, known as country with high level of organised crime due to corruption, arm trafficking, human trafficking or human rights violation, 4. state that is, based on assessment of the international organisation FATF (Financial Action Task Force) classified in to the non cooperative countries or territories (that are countries and territories that, according to FATF assessment, do not have relevant legislation in the area of prevention and detection of money laundering or terrorist financing, the state supervision of financial institutions does not exist or it is not relevant, establishing and acting of the financial institutions is possible without state certificates or registration at the competent authorities, state supports opening anonymous accounts or other anonymous financial instruments, the system of recognising and reporting suspicious transactions is inappropriate, the establishing beneficial owner is not an obligation prescribed by the law, international co-operation is not efficient or does not exists at all) 5. country against which UN or EU measures are imposed, including complete or partial break up of economic relations, railways, waterways, post, telephone lines, telegraph lines, radio and other communicational relations, breakup of diplomatic relations, military embargo, travel embargo etc. 6. country which is known as financial or tax paradise (for these countries it is particularly important that they enable complete or partial tax free obligation, or tax rate is significantly lower than tax rate in other countries. These countries usually do not have concluded agreements for the avoidance of double taxation, or if they do sign the agreements, they do not obey them. The legislation of these countries

	requires strict observance of bank and business secrecy and also quick, discreet and cheap financial services are provided. Countries known as financial or tax paradises are : Dubai – Jebel Ali Free Zone, Gibraltar, Hong Kong, Isle of Man, Lichtenstein, Macau, Mauritius, Monaco, Nauru, Nevis Island, Iceland –Norfolk Area, Panama, Samoa, San Marino, Isle of Sark, Seychelles, St. Kitts and Nevis, St. Vincent and Grenadine, Switzerland – canton Vaud and Zug, Turks and Caicos Islands, the USA – federal states Delaware and Wyoming, Uruguay, British Virgin Islands and Vanuatu 7. country known as offshore financial center (these countries define certain limitations in the process of direct activities registration of business entities in the country, provide high level of bank and business secrecy, liberal control over international trade business is performed, quick, discreet and cheap financial services and legal person registration are enabled. It is significant that these countries do no not have adopted relevant legislation in the area of prevention and detection of money laundering and terrorist financing. Countries known as offshore financial centers are: Andorra, Angola, Antigua and Barbuda, Aruba, Bahamas, Barbados, Belize, Bermudas, British Virgin Islands, Brunei Darussalam, Cape Verde, Cayman Islands, Cook Islands, Costa Rica, Delaware (USA), Dominica, Gibraltar, Grenada, Guernsey, Isle of Man, Jersey, Labuan (Malaysia), Lebanon, Lichtenstein, Macao, Madeira (Portugal), Marshall Islands, Mauritius, Monaco, Montserrat, Nauru, Nevada (USA), The Netherlands Antilles, Niue, Palau, Panama, Philippines, Samoa, Seychelles, St. Kitts and Nevis, St Lucia, St Vincent and Grenadines, Zug (Switzerland), Tonga, Turks and Caicos Islands, Uruguay, Vanuatu and Wyoming (USA). Transactions that could represent high risk of money laundering and terrorist financing include: 1. payment from customer's account or payment to customer's account, which differ from the account that customer provided in the process of identification of the account through which customer regularly carried or has been carrying business activities (particularly in case of crossbred transactions) 2. transactions intended to be sent to a persons with the residence or registered office in country known as financial or tax paradise, 3. transactions intended to be sent to persons with the residence or registered office in country known as off shore financial center, 4. transactions intended to be sent to non profit organisations with the registered office in: country known as off shore financial center, country known as financial or tax paradise or in non- EU member states, or country which did not sign EU Pre-Accession Agreement, Public statement under Step VI on MONEYVAL Compliance Enhancing Procedures in respect of Azerbaijan (12 December 2008) Public statement under Step VI of MONEYVAL's Compliance Enhancing Procedures in respect of Azerbaijan (24 September 2009)
(Other) changes since the last evaluation	Please see answer to question 1 in section "Special Questions" of this Questionnaire – relating to crucial substantive and procedural changes regarding the procedure of confiscation of property gain acquired through criminal offence (the procedure of permanent confiscation of property whose legal origin is not proved is introduced). Montenegro has accessed another very important convention in the field of international legal assistance – the European Convention on International Validity of Criminal Judgments (CETS 070). Having in mind that Montenegro has accessed the European Convention on Mutual Assistance in Criminal Matters with additional

	protocols, the European Convention on Extradition with additional protocols, the European Convention on Transfer of Convicted Persons with additional protocol, by confirming this convention Montenegro has completed the set of international instruments applied in the area of international legal assistance in criminal matters.

Special Recommendation VI (AML requirements for money/value transfer service)	
Rating: PC	
Recommendation of the MONEYVAL Report	*The requirements of Special Recommendation VI need to be implemented.*
Measures taken to implement the Recommendation of the Report	National payment system is regulated by the National Payment Systems Law (OGM 61/08), as well as by secondary legislation acts, among which, the following are particularly important with respect to the Special Recommendations VI and VII: - Decision on the structure of transfer execution account and the detailed conditions and manner of account opening and closing (OGM 24/09); - Decision on unified structure for identification and classification of accounts using IBAN standard for international payments (OGM 24/09), - Decision on minimum elements of credit and debit order (OGM 24/09), - Decision on conditions and manner of performing individual transfer execution by agents (OGM 24/09); - Decision on the issuing and use of remote access instruments and the reporting manner and timelines (OGM 24/09), - Decision on detailed conditions of issuing and revoking licenses for payment system and granting approvals (OGM 24/09), - Decision on payment system oversight (OGM 24/09), - Payment system rules for interbank transfer execution (OGM 24/09). The National Payment Systems Law governs the performance of national payment system: transfers of funds, settlement of inter-bank transfers, electronic payment instruments and payment systems and out-of-court settlement of payment system-related disputes. Transfer of funds, under this Law, shall be a transfer of monetary assets executed at the originator's order by the performing institution. International payment system operations are regulated by the External Current and Capital Transactions Law (OGM 45/05 and OGM 62/08). This Law regulates the performance of payment operations between residents and non-residents in euro and currency other than euro, as well as the manner for transfer of property to Montenegro and out of Montenegro, and the capacity of residents to have ownership over means of payment denominated in currency other than euro. According to Montenegrin legislation (Banking Law, OGM 17/08, National Payment Systems Law, and External Current and Capital Transactions Law), the transfer of funds in the country and abroad is performed exclusively by legal persons, primarily banks, foreign bank branches and other legal persons that have obtained license or approval for transfer execution by the Central Bank. The National Payment Systems Law additionally regulates agents as legal persons that may be entrusted by the performing institution, in accordance with the appropriate agreement, certain activities related to the execution of a transfer. The agent performs these activities in the name of and for the account of the performing institution that is responsible for all the agent's procedures and failures arising from the performance of the aforesaid activities.

	The Central Bank has up-to-date records on all service providers of transfer of funds. As described in point VI.1, the work of an agent, as a legal person to whom the performing institution has entrusted, in accordance with the appropriate agreement, certain activities related to the execution of a transfer is regulated by the National Payment Systems Law and Decision on conditions and manner of performing individual operations in transfer of funds execution by agents. Only Post Office of Montenegro is currently acting as an agent of the payment system in Montenegro. The aforesaid Decision regulating the work of agents is the act passed by the Central Bank of Montenegro, which will incorporate this requirement.
Recommendation of the MONEYVAL Report	*The Montenegrin authorities should introduce legislation to enforce the licensing/registration of all MVT service providers together with appropriate sanctions.*
Measures taken to implement the Recommendation of the Report	See the answer presented in the first part of SR VI.
(Other) changes since the last evaluation	

Special Recommendation VII (Wire transfer rules)	
Rating: NC	
Recommendation of the MONEYVAL Report	*The requirements of Special Recommendation VII should be incorporated into the legislation of Montenegro.*
Measures taken to implement the Recommendation of the Report	Decision on the structure of transfer execution accounts and the detailed conditions and manner of account opening and closing (OGM 24/09) regulates, *inter alia*, opening and closing of transfer execution accounts in the country. The following data should be mentioned, *inter alia*, by the client in his application: - Name of the legal or natural person that performs registered activity, i.e. name and last name of natural person not performing registered activity, - Place – registered office or residence, address and phone number; - Identification number of legal or natural person performing registered activity or uniform identification number of citizens for natural person not performing registered activity and the like. In that respect, requested information on ordering party of electronic transfer in any transfer amount. The aforesaid is valid in situations when the cash payment of natural person precedes the transfer (e.g. cash payment by various accounts or any other basis). The account of the financial institution (bank) that simultaneously processes that transfer appears as the account of originator (ordering party) of such transfer. The Decision on minimum elements of credit and debit order prescribes the obligatory elements that these payment instruments must contain to initiate electronic transfers. The minimum prescribed elements includes also payment orders submitted electronically. In accordance with Articles 7 and 8 of the Decision, transfer should also contain the

	following in order to be executed,: - name of the originator as ordering party, i.e. name and registered office of legal or natural person performing registered activity or name, last name and address of residence of natural person not performing registered activity, and – debited or credited account. If the cash payment by natural person of such transfer preceded the transfer, the financial institution (bank) simultaneously processes that transfer, so the account of institution that debits the account is also mentioned. Pursuant to Article 16 of the National Payment Systems Law, the performing institution is obliged to archive the documentation on executed transfers and store them for five years, and to keep the electronic data on executed transfers for ten years from the date of the execution of the transfer. When developing risk analysis for money transfers, banks and/or financial institutions shall define in their internal acts, based on the Guidelines on bank risk analysis aimed at the prevention of money laundering and terrorism Financing, the criterion that will have high risk concerning electronic transfer that do not contain complete information on ordering party. Transfers without complete information on ordering party and related transactions shall be considered suspicious and shall be acted upon the prescribed manner, and in some cases, the termination of business relations shall be performed with the financial institutions not complying with standards referred to in Recommendation VII. Banks in Montenegro as bearers of national and international payment systems shall, pursuant to Articles 7 and 71 of the LPMLTF, identify client (legal or natural person) prior to execution of transaction and obtain all prescribed data and/or following data and information: - name of the company, address, registered office of the company and personal identification number of the legal person, that establishes business relationship or executes transaction, or legal person for whom is established business relationship or executed transaction; - name, address of permanent residence or temporary residence, date and place of birth and tax ID number of a representative or an authorised person, that for a legal person or other juristic person conclude the business relationship or execute transaction, number, kind and name of the authority that issued the personal documents; - name, address of permanent residence or temporary residence, date and place of birth and tax ID number of an authorised person, which requires or executes transaction for a costumer, and number, kind and name of the competent body that issued the personal documents; - name, address of permanent residence or temporary residence, date and place of birth and tax ID number of natural person or tax ID number of its representative, entrepreneur or natural person carrying out activities, and that establish business relation ship or execute the transaction, or natural person, for which is established business relationship or executed transaction, and number, kind and name of the competent body that issued the personal documents; - date and time of executing transaction ; - the amount of transaction and foreign currency of transaction that is executed; - the purpose of transaction and name and address of permanent residence or temporary residence, registered office of the company and residence of the person to which transaction is intended; - method of executing the transaction; - data on assets and income sources, that are or will be the subject of transaction or

	business relationship. Pursuant to Article 86 and with respect to Article 4 points 1, 2, 3, 10 and 13 of the LPMLTF, the Central Bank oversees the implementation of this law and enabling regulations and imposes measures against banks violating LPMLTF.
(Other) changes since the last evaluation	

Special Recommendation VIII (Non-profit organisations)	
Rating: NC	
Recommendation of the MONEYVAL Report	*Montenegro should conduct a review of the adequacy of its legal framework that relates to NPOs that can be abused for terrorism financing.*
Measures taken to implement the Recommendation of the Report	No significant measures have been taken
(Other) changes since the last evaluation	**Normative framework** The Law on Non-Governmental Organisations (Official Gazette of Montenegro No. 11/07), regulates the issues of procedure, registration, terms and forms of associations of citizens in Montenegro. Non-governmental organisations shall be non-governmental associations and non-governmental foundations. A non-governmental association is defined as 'a nonprofit organisation with members, founded by domestic and foreign physical persons and legal entities, in order to realise individual or common interests or for realisation and affirmation of public interest.' A non-governmental foundation is 'a nonprofit organisation without members, founded by domestic and foreign physical persons and legal entities, for pooling resources and assets in order to realise charitable and other activity, which are of public interest and importance.' According to the provisions of this Law, non-governmental organisations are not political organisations, religious communities, trade union organisations, sport organisations, business associations, and organisations and foundations whose founder is the State. The changes and amendments of the Law on NGOs from 2007 precisely define the terms under which an NGO can perform its business activity. Certain issues related to the operating of NGOs are regulated by other laws: The Law on Tax on Profit of Legal Persons (Official Gazette MNE No. 80/04) defines non-taxable profit of NGOs; Law on Administrative Taxes (Official Gazette MNE No. 80/04) that liberates NGOs from paying taxes and fees for accomplishing the goals they are set for; Law on Value Added Tax (Official Gazette MNE No.80/04) that, under certain conditions, liberates from paying taxes of NGOs services; Law on Property Sales Tax (Official Gazette MNE No. 80/04) prescribes that this tax shall not be paid by NGOs for the real estates they use for performing the activities they are founded for; Law on State Administration (Official Gazette MNE No. 38/03) and Law on Local Self-Government (Official Gazette MNE No.13/06) regulate the relations between the state administration authorities, or local self-government authorities and NGOs. These laws define the obligation of

	appropriate consulting of NGOs in the procedure of preparing and adopting laws, bylaws and other regulations and enactments, as well as development projects and programs; Law on Games of Chance (Official Gazette MNE No. 52/04) prescribes that a part of the profit from games of chance shall be used for financing the projects of NGOs and other organisations, and the Government adopted the Bill on Changes and Amendments of the Law on Games of Chance, that precisely defines the amount of at least 75% of the profit from games of chance that shall be used for financing the plans and programs of NGOs and other organisations. 4200 NGOs are registered in Montenegro (the number has the tendency of growth, and it has been changing on daily basis). The registration and the register of NGOs are kept by the Ministry of Interior Affairs and Public Administration. The financing made by the state is done in accordance with the Law on NGOs and the Law on Games of Chance through public announcements, and the decisions are made by the Commission of the Montenegro Parliament and the Government Commission established in accordance with these laws. **Institutional framework** In the beginning of 2007 the Government of Montenegro established the Office for Co-operation with NGOs, which functions as an internal organisational unit of the General Secretariat of the Government.
Recommendation of the MONEYVAL Report	*Montenegro should implement measures to ensure that terrorist organisations cannot pose as legitimate NPOs.*
Measures taken to implement the Recommendation of the Report	No significant measures have been taken
Recommendation of the MONEYVAL Report	*Montenegro should also reach out to the NPO sector with a view to protecting the sector from terrorist financing abuse. This outreach should include i) raising awareness in the NPO sector about the risks of terrorist abuse and the available measures to protect against such abuse; and ii) promoting transparency, accountability, integrity, and public confidence in the administration and management of all NPOs.*
Measures taken to implement the Recommendation of the Report	No significant measures have been taken
Recommendation of the MONEYVAL Report	*Montenegro should take more proactive steps to promote effective supervision or monitoring of NPOs. Authorities should ensure that detailed information on the administration and management of NPOs are available during the course of an investigation or on request internationally. Montenegro should also implement effective sanctions for violations of oversight measures or rules by NPOs or persons acting on behalf of NPOs.*
Measures taken to implement the Recommendation of the Report	The Administration for the Prevention of Money Laundering and Terrorist Financing, within its defined competences, supervises humanitarian organisations, NGOs and NPOs regarding the implementation of the LPMLTF and the bylaws adopted upon this Law. The supervision is carried out through the compliance officer, in accordance with the law regulating the issue of supervision
(Other) changes since the last	

evaluation	

Special Recommendation IX (Cross Border declaration and disclosure)	
Rating: PC	
Recommendation of the MONEYVAL Report	*The Customs Administration should be given clear powers to stop individuals and restrain currency in all circumstances.*
Measures taken to implement the Recommendation of the Report	The customs control of cross border money transferring is prescribed by the following: • Law on Foreign Current and Capital Operations ("Official Gazette of the Republic of Montenegro, No. 45/05, 62//08), • Decision on the amount of cash that can brought in or out of the Republic of Montenegro without declaring- Official Gazette of the Republic of Montenegro, No.58/05), • Law on the prevention of money laundering and terrorist financing ("-Official Gazette of the Republic of Montenegro, No.14/07, 4/08) • Rulebook on the Manner of Reporting Cash Transactions exceeding €15,000 or more and Suspicious Transactions to theAdministration for the Prevention of Money Laundering and Terrorist Financing (Official Gazette of the Republic of Montenegro, No. 79/08). In accordance with valid regulations, residents and non-residents are obligated to report physical bringing in or out of currency at place of entry or exit to/from Montenegro. Physical persons, Le. residents and non-residents, in passengers traffic with foreign countries, can bring in or out the amounts up to 2000 € (in euro or other currency) without reporting it to the customs authorities. The amount exceeding 2000 € is reported to the border customs authority. Pursuant to the Article 66 of Law the Customs Administration is obligated to submit to the Administration for the prevention of anti-laundering information on every cross-border transport of money, checks and bearer negotiable instruments, precious metal and precious stones, in value exceeding 10,000 Euro, within 3 days following the cross-border transport. (Official Gazette of Montenegro 14/07). In accordance with the above Law, Customs Administration is obligated to submit to the Administration for the prevention of anti-laundering information on every cross-border transport or attempt to transfer money, checks and bearer negotiable instruments, precious metal and precious stones, in value below 10,000 Euro, if there is a suspicion of money laundering or terrorism financing. Reporting forms, which we previously used, was addendum to the Agreement on co-operation between the Administration for the Prevention of Anti-laundering and Terrorism Financing and the Customs Administration, from October 2004. Since 31 December 2008 when the Rulebook on providing data on cash operations of value of or exceeding 15,000 € and suspicious transactions to the Administration for Prevention of Money-laundering and terrorism financing entered into force (Official Gazette of Montenegro 79/08) we are using new form - FORM 06 for Customs authorities, which was printed together with the Rulebook and represents its integral part.
Recommendation of the MONEYVAL Report	*The Customs Administration should have the legal authority to restrain currency in cases of an administrative offence.*

Measures taken to implement the Recommendation of the Report	Valid legal regulations (Law on Foreign Current and Capital Operations, Official Gazette of the Republic of Montenegro 45/05, 62/08, Official Gazette of Montenegro 62/08, Decision on the amount of cash that can be brought in or out of the Republic of Montenegro without declaring- Official Gazette of the Republic of Montenegro 58/05, Law on Prevention of Money-laundering and terrorism financing - Official Gazette of Montenegro 14/07, 4/08, Rulebook on providing data on cash operations of the 15,000 € value or more and suspicious transactions to the Administration for Prevention of Money-laundering and terrorism financing Official Gazette of Montenegro 79/03) prevent Customs Administration to keep funds in the cases of administrative offences. During the period 1 March 2009 - 31 December 2009, Customs Administration had four cases of non-declaring currency by persons entering or exiting territory of Montenegro. In all four cases, persons who didn't declare the currency to the customs authority were fined in accordance with Article 15, Paragraphs 1 and 3 of the Law on Foreign Current and Capital Operations, with adequate pecuniary fines. During the period from 1 March 2009 - 31 December 2009, Customs Administration has forwarded 144 reports on transport of money, checks and bearer negotiable instruments, precious metal and precious stones, as divided per months: March- 14, April- 16, May - 16, June - 19, July - 15, August - 11, September - 19, October - 11, November - 9 and December - 14. Also, during the period 1 March 2009 - 31 December 2009, Customs Administration has provided information on 26 instances on suspicious transactions to the Administration for the Prevention of Anti-laundering and Terrorism Financing .
Recommendation of the MONEYVAL Report	*The Customs Administration should take into consideration a system to use reports on currency declaration in order to identify money launderers and terrorists.*
Measures taken to implement the Recommendation of the Report	Customs administration is keeping records of all reports made by all customs officers on the territory of Montenegro, which is later forwarded to the Administration for the prevention of anti-laundering. In case of suspicion of money laundering, regardless of amount of cash, or value of checks and bearer negotiable instruments, precious metal and precious stones, transported across the border, the customs officer at border crossing is obligated to immediately inform the officers in Customs Enforcement sector. Afterwards, the information, i.e. the report, using the same form is submitted to the Customs Enforcement sector, which shall forward it to the Administration for the prevention of anti-laundering, within 3 days from transport, as legally required. Pursuant to the Article 69 of Law on prevention of money laundering and terrorism financing, Customs Administration is obligated to inform the Administration for the prevention of anti-laundering information on annual basis, and until the end of January at the latest, on its observations and undertaken activities related to the transactions suspicious of money laundering or terrorism financing. Articles 74 and 75 of this Law prescribed the records, which the Customs Administration is obligated to keep, as well as its contents. The Customs Administration is obligated to keep the records for 11 years after its collection, and such information is being destroyed after the expiry of that deadline.
Recommendation of the MONEYVAL Report	*The administrative sanctions for false declarations or non-declared currency should be raised considerably. Taking into account the low chance of detection, the fines are not considered to be dissuasive or effective.*

Measures taken to implement the Recommendation of the Report	All the cases of finding currency that was not declared at the moment of crossing border are processed to the competent organisational unit of the customs administration and the offenders are sentenced administrative fines, pursuant to the Article 15 of the Law on Foreign Current and Capital Operations, which lay down the amount of fine.
Recommendation of the MONEYVAL Report	*In order to increase its effectiveness, the Customs Administration should hire more specialised staff to deal with money laundering and terrorist financing cross-border transportation of currency.*
Measures taken to implement the Recommendation of the Report	Customs Administration in 2009 continued with comprehensive training of customs officers in the area of money laundering and terrorism financing. Customs officers working in customs offices at the border or at airports, together with officers from the Department of prevention of smuggling that belong to headquarters and two officers appointed in accordance with Article 1 of the Agreement between the Administration for the prevention of anti-laundering and Customs Administration, to act as liaison officers and official contact points for the Administration for the prevention of anti-laundering, are employees of customs administration involved in control of bringing in or out of domestic or foreign currency. We would like to note that positive legal regulations are defining the amount of administrative fines for false impersonation or non-declaring currency, and that it prevents the Customs Administration from withholding funds from fines in cases of administrative offences, and provide recommendations in the section related to amendment of existing legal acts in jurisdiction of the Ministry of Finance. In the period from 1st March to 31st December 2009 the Customs Administration had four cases of non declaring cash by persons entering and leaving the territory of Montenegro. In all four cases persons that failed to declare money are penalized, by appropriate fines, in accordance with Article 15 paragraph 1 and 3 of the Law on Foreign Current and Capital Operations. Since 31st December 2008 when the Rulebook on the Manner of Reporting Cash Transactions exceeding €15,000 or more and Suspicious Transactions to the Administration for the Prevention of Money Laundering and Terrorist Financing, the Customs Administration uses the new form (Form 06 for customs authorities) and it is the integral part of the Rulebook.
(Other) changes since the last evaluation	

4. Specific Questions

1. Have any steps been take to introduce a reversal of the burden of proof regarding property subject to confiscation?

In August 2009, the Parliament of Montenegro adopted new Criminal Procedure Code (Official Gazette of Montenegro no 57/09) in which it is prescribed reversed burden of proof in order to extend confiscation of the property (confiscation of property whose legal origin has not been proved). In the article 486-489 of the CPC it is prescribed

„*after the finality of the judgment finding the accused person guilty of the criminal offence for which Criminal Code prescribes the possibility of extended confiscation of property from the convicted person, his legal successor or the person to whom the convicted person has transferred the property and who cannot prove the legality of its origin, the State Prosecutor shall, at the latest within one year, submit the request for the confiscation of the property of the convicted person, his legal successor or the person to whom the convicted person has transferred the property for which there is no evidence on the legality of its origin.*"

Those articles in the CPC are procedural norms and for their implementation there is a need for the change of the existing Criminal Code and to have the institute of extended confiscation of property. According to this, in the proposal of the changes of Criminal Procedure Code there are three new paragraphs and the Article 113 is now:

„ (1) Money, things of value and all other property gains obtained by a criminal offence shall be confiscated from the offender; should such a confiscation be not possible, the perpetrator shall be obliged to pay for the monetary value of the obtained property gain.

(2) property for which there is founded suspicion that derives from the criminal activity shall be confiscated form the offender unless the offender makes it probable legality of its origin (extended confiscation)

(3) Confiscation from the paragraph 2 of this Article can be applied if the offender is finally convicted for
-some of the criminal offence from the Article 401 a of this Code that was committed within the criminal organisation;

- some of the following criminal offences:
1) terrorism
2) Non authorised production, keeping and releasing for circulation of narcotics;
3)against payment operations and economic transactions and against official duty committed out of lucrative for which it is the penalty of 8 years or more of the imprisonment can be imposed

(4) Property from the paragraph 2 of this article can be confiscated if it is gained from the criminal activity in the period of 5 years before the committing the crime from the paragraph 3 of this article and/or after committing criminal offence until the judgment is final.

(5) A material gain obtained by a criminal offence shall also be confiscated from the persons it has been transferred to without compensation or against compensation that is obviously inadequate of its real value
(6) Confiscated shall also be any property obtained by a criminal offence in favor of other persons."

2. Since the on-site visit, have any steps been taken to expand access by the APMLTF to other authorities databases?

The APMLTF, Police Directorate, Department of Public Revenues and Customs Directorate, with the help of: OSCE Mission to MNE, Customs and Fiscal Assistance Office (EU) – CAFAO, United Nations Office on Drugs and Crime – UNODC, Swedish National Police Board, International Criminal Investigative

Training Assistance Program – ICITAP, US Embassy and British Embassy, harmonised the model of joint office for coordination and intelligence data exchange- with working title " National coordination office for the state administration. The Working group adopted the Conclusion that the conditions for establishing this office are fulfilled and send the letter to the Prime Minister of Montenegro (directors of all involved state administration authorities has signed this letter) suggesting the specific measures. The Prime minister has forwarded the suggestion to the Ministry of Internal Affairs and Public Administration so that the national office could be established. The establishing of this office will enable data exchange between: the Administration for the Prevention of Money Laundering and Terrorist Financing, Police Directorate, Department of Public Revenues and the Customs Administration
Department of Public Revenues possesses appropriate software and data base that enables collecting, analysing and forwarding data. This data base is upgraded continuously and upon the appropriate requests is available to all authorities involved in the system of prevention of money laundering and terrorist financing .

3. Has an updated list of suspicious transaction indicators been issued to obligors? If so, when was the list last updated? Furthermore, does APMLTF now provide regular general feedback to all obligors containing:

(a) statistics on the number of disclosures, with appropriate breakdowns, and on the results of the disclosures;

(b) information on current techniques, methods and trends (typologies); and

(c) sanitised examples of actual money laundering cases.

Yes .
Rulebook on Indicators for recognising suspicious clients and transactions ("Official Gazette of Montenegro " No. 69/09, from 16th October 2009) adopted by Ministry of Finance and due to that the following List of indicators for recognising suspicious clients and transactions was established :
- List of Indicators for banks,
- List of Indicators for capital market,
- List of Indicators for the Customs Administration,
- List of Indicators for the Department of Public Revenues,
- List of Indicators for leasing companies,
- List of Indicators for auditors,
- List of Indicators for accountants,
- List of Indicators for lawyers and
- General indicators.

Department of Public Revenues, in relation to risk assessment on money laundering and terrorist financing and instructions sent to the inspection control subsidiaries, obliged the tax inspectors to check the origin, purpose of the business relationship and transaction in accordance with the List of Suspicious Transactions Indicators, to the greatest extent possible. The real-estate and construction sectors are designated as specific sectors.

Furthermore, does APMLTF now provide regular general feedback to all reporting entities containing:

The APMLTF provides information, in written form, to the reporting entity or other requester, on obtaining and analysing data, information and documentation related to persons or transactions for which there are reasonable grounds for suspicion in criminal offence of money laundering or terrorist financing except in case when it is assessed that such informing could have harmful effects for the process and outcome of the procedure .

APMLTF provides feedback on results of the actions that are undertaken upon the STRs submitted by reporting entities. For the purpose of data confidentiality and data secrecy the feedback breakdown is given in statistical form. The breakdown is made in total and individually for each reporting entity. It includes the number of analytical cases opened on the basis of STRs.

In 2009 the APMLTF has sent 38 feedback information to the reporting entities and in 2010 three information are sent.

2009

Commercial Banks	42 feedback information
Lawyers	1 feedback information
Capital city of Podgorica	1 feedback information
SEC	2 feedback information

2010

Securities Commission	1 feedback information
Insurance company	1 feedback information
Customs administration	1 feedback information

(a) statistics on the number of disclosures, with appropriate breakdowns, and on the results of the disclosures;

(b) information on current techniques, methods and trends (typologies);

APMLTF established, based on analysis, money laundering typologies that are presented to the compliance officers and employees with the reporting entities that have a direct contact with customers.
The following business activities are designated, on the basis on present experience, as high risk areas from the aspect of money laundering and terrorist financing :

- Real-estate trade,
- Construction business,
- Service providing companies,
- Capital market,
- Organisers of games of chance
- Sport organisations

In relation to the above mentioned business activities, APMLTF processed cases related to numerous legal and natural persons, residents and non-residents, and achieved a significant co-operation with foreign FIUs. After analysis performed these cases are forwarded to the competent state authorities or foreign FIUs.
According to feedback information, the significant number of cases resulted with police investigations, bringing indictments for the criminal offence of money laundering and other criminal offences and final court decisions for other criminal offences related to money laundering.
Real-estate trade:

- Fictitious contracts– contract cancellation right after concluding the contract. Presenting the same land parcels as the subject of sale in the contract and under the different conditions.
- Fictitious contracts where unreal –false price is presented in the contract or by direct bargain between seller and buyer where seller consent not to record the status in ownership change at the ownership registry (obtaining property rights is not recorded)
- Founding capital increase without recording changes of the status documentation at the Commercial Court (provision of the Law) and afterwards withdrawing cash from the account in the same amount (deposited).

Construction business:

- This business activity is related to the real estate trade.
- Using cash for constructing buildings
- Making contract on selling buildings that are neither constructed nor in the starting phase of construction.
- Fictitious Companies
- Illegal founding of legal persons
- Parallel – linked companies (the same persons are founders and representatives)
- Non existing companies
- Non available companies (nonresidents)
- Transactions that do not correspond with the business activity for which the company is registered by the range of business activity or natural person does not have a company and the natural person is unemployed but on its account are recorded enormous inflows without the clear purpose of transaction.

*(I Case study from practice: 2 resident and 2 non resident natural persons from the neighbor country. The case is forwarded to the Police directorate and State Prosecutor's Office and afterwards assets were confiscated and natural persons were arrested. There was a significant co-operation with the foreign FIU.
A natural person, without criminal records, has been engaged by criminal group and (with benefits) this natural person is used for opening account and enormous inflows from abroad and afterwards withdrawal and cash payments to the members of this criminal group in order to conceal the trace .
*(II Case study related to alleged spot managers when high amounts were sent from abroad for football transfers. There was a significant co-operation with the foreign FIU. The FIU confirmed that the case has been pursued and that our information was used in the court process.
(III Case study : presenting enormous amounts as alleged prize from games of chance (betting house) The case has been pursued.

- Loans from companies
- Magnified invoice value(disproportional expenses)
- In relation to the capital market :
- Block businesses

These business activities are used with the aim of justifying the origin of money that would be gained by sail (on the capital market), after direct agreement between stock exchange market clients(buyer and seller) about the stock price and in the manner that the price would be unrealistically high or low.

Services providing companies
- TAXI associations (registration of unrealized profit from providing services) delivered to the Department of Public Revenues and APMLTF due to reasonable grounds of suspicion in other criminal
- Catering companies (forwarded to the Tax Administration) registration of unrealized profit from providing goods and services

Transferring non-declared TRAVELLERS checks (amounts in million of euros) across the state border and attempt of converting checks at banks in Montenegro. This case has been forwarded to the Police Directorate) and
(c) sanitised examples of actual money laundering cases.
At trainings, seminars and round tables organised by APMLTF case studies and sanitised examples are jointly presented and analysed.

4. Please explain the arrangements for co-operation between policy makers, FIU, law enforcement and supervisory bodies at a strategic level. At the operational level, have additional formal agreements been concluded in order to define the type of information to be exchanged, timeliness of the exchange, the names of contact person, etc.?

On 19th February 2010 APMLTF, Supreme State Prosecutor's Office, Police Directorate Department of Public Revenues and Customs Administration signed the MoU in prevention and prosecution of offenders related to organised crime and corruption. The MoU defines obligations, general rules and terms of

forming and working of the joint team that will act in special cases of organised crime and corruption. The team, whose work will be coordinated by the Supreme State Prosecutor, is composed of representatives of APMLTF, Supreme State Prosecutor's Office, Police Directorate Department of Public Revenues and Customs Administration, who will be appointed for the period of three years.
With a view to establishing better co-operation between the Supreme State Prosecutor's Office and Police Directorate, and according to the evaluators' recommendations, the Memorandum on Understanding and information exchange related to prevention, detection and prosecution of offenders prosecuted ex officio.
The Memorandum refers to co-operation and acting in pre-trial criminal and criminal procedure, especially to:
1. direct communication between the competent state prosecutor and the competent officer of the Police Directorate
2. forming ad hoc joint teams for complex investigations
3. ensuring procedure and data secrecy
Signing the Memoranda of understanding related to preventing, detecting and prosecuting the offenders in the area of organised crime and corruption, is planned and it will be signed by State Prosecutor's Office, Police Directorate, APMLTF, Department for Public Revenues and Customs Administration.
Signing the memoranda of understanding between the APMLTF and Deposit Protection Fund is planed as well as innovation of the MoU between APMLTF and CBM. There are designated representatives of these institutions that will prepare the text of the new MoU.

On the basis of analysing the assessment of needs for concluding new bilateral Memoranda, the APMLTF has, for the forthcoming period, planned innovating memoranda with Central Bank of Montenegro(CBM) and signing the new memoranda with the supervising authorities from Article 86 of the LPMLTF . In March 2009 the APMLTF signed MoU with the State Audit Institution of Montenegro. Previously signed MoUs between the APMLTF and Customs Administration, Securities Commission, Ministry of Interior and Public Administration, Department for Public Revenues, CBM and basic Court in Podgorica, are fully applied. The co-operation with the Police Directorate and State Prosecutor's Office is achieved through daily communication.

The establishment of the National coordination office for the state administration is in progress.
The time period for exchange of information is prescribed by the LPMLTF, Article 50 of the LPMLTF:
State authorities and public powers holders shall provide the requested data, information and documentation to the competent administration body without delay, and not later than eight days after the day of receiving the request, or enable, without compensation, direct electronic access to data and information stated in the request.

(In relation to supervision Article 89 of the LPMLTF „Bodies from Article 86 of this law shall inform the competent administration body on measures taken in process of supervising in accordance with this Law, and within 8 days from the date on which the measures were taken.)

The APMLTF and Ministry of Interior agreed, due to MoU signed in 2004, that in these institutions shall be designated an officer and its deputy that will be the official contact person for co-operation between these institutions.

On 17th February 2009 Securities commission signed IOSCO Multilateral Memorandum of Understanding Concerning Consultation and Co-operation and the Exchange of Information. With signing this memorandum Securities and Exchange Commission become included into the international network of supervisors and provided a significant asset in acting upon taking measures on the international level. Signing this MoU shows the capability of the Securities and Exchange Commission to ensure harmonisation with regulations and full implementation of regulations related to securities. Also, the MoU confirms capacities and readiness of the Securities and Exchange Commission to provide the greatest

possible assistance to the international regulators of the securities market in order to facilitate their work on the securities market. Signing this MoU is a significant step for SEC since it enables the Commission to exchange information with all relevant world wide jurisdictions and leads Montenegro to full compliance with best international practice. The SEC drafted the proposal of the memorandum with CBM and drafting the proposal with the ISA is underway. ISA has not signed the MoUs with the competent authorities from the LPMLTF. The activities on signing the mentioned are one of the priorities of ISA in 2010. The Customs Administration signed the MoU with the Faculty of Law in Podgorica (training employees)
5. Have provisions been introduced to ensure that the names and personal details of staff of financial institutions that make a STR are kept confidential by APMLTF?
Article 55, paragraph 2 of the LPMLTF defines as follows : In notification from paragraph 1 of this Article the competent administration body shall not state data on reporting entity and on person employed in the organisation, that announced data unless there are reasonable grounds for suspicion that reporting entity or reporting entity's employee committed criminal act of money laundering or terrorist financing, or if those data are necessary for establishing facts in criminal proceedings and if transferring those data are required, in written form, by Court. Article 80, paragraph 2 and 3 of the La won PML/TF defines The information about the facts from paragraph 1 of this Article and notification on suspicious transactions or information about other offences from Articles 55 and 56 of this Law, are the official secret and designated as such, in accordance with Law. On removing the official secret designation, from paragraph 2 of this Article shall decide the authorised person of the administration.

5. Questions related to the Third Directive (2005/60/EC) and the Implementation Directive (2006/70/EC)[3]

Implementation / Application of the provisions in the Third Directive and the Implementation Directive	
Please indicate whether the Third Directive and the Implementation Directive have been fully implemented / or are fully applied and since when.	Yes in the Law on the Prevention of Money Laundering and Terrorist Financing

[3] For relevant legal texts from the EU standards see Appendix II.

Beneficial Owner	
Please indicate whether your legal definition of beneficial owner corresponds to the definition of beneficial owner in the 3rd Directive[4] (please also provide the legal text with your reply)	**LPMLFT /Establishing the Beneficial Owner** **Beneficial Owner** **Article 19** In the context of this Law the following shall be considered as a beneficial owner of a business organisation or legal person: 1. a natural person who indirectly or directly owns more than 25% of the shares, voting rights and other rights, on the basis of which he/she participates in the management, or owns more than a 25% share of the capital or has a dominating influence in the assets management of the business organisation, and 2. a natural person that indirectly ensures or is ensuring funds to a business organisation and on that basis has the right to influence significantly the decision making process of the managing body of the business organisation when decisions concerning financing and business are made. Also, a business organisation, legal person, as well as an institution or other foreign legal person that is directly or indirectly a holder of at least €500,000 of shares, or capital share, shall be considered a foreign owner. As a beneficial owner of an institution or other foreign legal person (trust, fund and the like) that receives, manages or allocates assets for certain purposes, in the context of this Law, shall be considered: 1. a natural person, that indirectly or directly controls more than 25% of a legal person's asset or of a similar foreign legal entity, and 2. a natural person, determined or determinable as a beneficiary of more than 25% of the income from property that he/she manages. **Establishment of a beneficial owner of a legal person or foreign legal entity** **Article 20** An reporting entity shall establish the beneficial owner of a legal person or foreign legal person by obtaining data from Article 71 item 15 of this Law. An reporting entity shall obtain the data from paragraph 1 of this Article by checking the original or certified copy of the documentation from the CRCC or other appropriate public register that may not be older than three months of its issue date or obtain them on the basis of the CRCC or other public register in accordance with Article 14 paragraphs 3 and 5 of this Law. If the required data cannot be obtained in the manner determined in paragraphs 1 and 2 of this Article, an reporting entity shall obtain the missing data from a written statement of an agent or authorised person. Data on beneficial owners of a legal person or similar foreign legal entity shall be verified to the extent that ensures complete and clear insight into the beneficial ownership and managing authority of a customer respecting risk-degree assessment.

Risk-Based Approach	
Please indicate the extent to which financial institutions have been permitted to use a risk-based	The LPMLTF prescribes in Article 13 transactions that do not require the application of customer due diligence measures, which reads: "Insurance companies conducting life insurance business and business units of foreign insurance companies licensed to conduct life insurance business Montenegro, founders, managers of pension funds, and legal and natural persons conducting representation and brokerage business in insurance, when entering into

[4] Please see Article 3(6) of the 3rd Directive reproduced in Appendix II.

approach to discharging certain of their AML/CFT obligations.	life insurance contracts do not need to conduct the verification of a customer when: 1) entering into life insurance contracts where an individual installment of premium or multiple installments of premium, payable in one calendar year, do not exceed the amount of €1,000, or where the payment of a single premium does not exceed the amount of €2,500; 2) concluding pension insurance business providing that it is: - insurance within which it is not possible to assign the insurance policy to a third person or to use it as security for a credit or borrowing, or - a conclusion of a collective insurance contract ensuring the right to a pension. Domestic and foreign companies and business units of foreign companies that issue electronic money do not need to conduct the verification of a customer when: 1)issuing electronic money, if the single maximum value issued on the electronic data carrier, upon which it is not possible to re-deposit value, does not exceed the amount of €150, and 2)issuing and dealing with electronic money, if the total amount of value kept on the electronic data carrier, upon which it is possible to re-deposit value, and which in the current calendar year does not exceed the amount of €2,500, unless the holder of electronic money in the same calendar year cashes the amount of €1,000 or more. An reporting entity does not need to conduct control over a customer to whom it provides other services or related transactions representing an insignificant risk of money laundering or terrorist financing, unless there are reasonable grounds for suspicion of money laundering or terrorist financing. Cases representing an insignificant risk of money laundering or terrorist financing shall be more specifically regulated by a regulation of the Ministry." Simplified customer verification is prescribed in Article 29 of the LPMLTF, which reads: "Unless there are reasonable grounds for suspicion of money laundering or terrorist financing in relation to a customer or transaction from Article 9 paragraph 1 items 1 and 2 of this Law, an reporting entity can conduct simplified verification of a customer that is: 1)the reporting entity from Article 4 paragraph 2 items 1, 2, 4, 5, 6, 8 and 9 of this Law or other appropriate institution that has a registered office in the EU or in a state from the list; 2)state body or local governance body and other legal persons exercising public powers; 3)an organisation whose securities are included in the trade on the organised market in the EU member states or other states where the EU standards are applied on the stock markets, and 4)the customer from Article 8 paragraph 4 of this Law to whom an insignificant risk of money laundering or terrorist financing is related. The list of the states from paragraph 1 of this Article shall be determined by the Ministry."

Politically Exposed Persons	
Please indicate whether criteria for identifying PEPs in accordance with the provisions in	Article 27 of the LPMLTF determines the following PEPs definition: A natural person that is acting or has been acting in the last year on a distinguished public position in a state, including his/her immediate family members and close associates, shall, in the context of this Law, be considered politically exposed person, as follows: 1. presidents of states, prime ministers, ministers and their deputies or assistants, heads of administration authority and authorities of local governance units, as

the Third Directive and the Implementation Directive[5] are provided for in your domestic legislation (please also provide the legal text with your reply).	well as their deputies or assistants and other officials; 2. elected representatives of legislative authorities; 3. holders of the highest juridical and constitutionally judicial office; 4. members of State Auditors Institution or supreme audit institutions and central banks councils; 5. consuls, ambassadors and high officers of armed forces, and 6. members of managing and supervisory bodies of enterprises with majority state ownership. Marital or extra-marital partner and children born in a marital or extra-marital relationship and their marital or extra-marital partners, parents, brothers and sisters shall be deemed immediate family members of the person from paragraph 1 of this Article. A natural person that has a common profit from the asset or established business relationship or other type of close business contacts shall be deemed a close assistant of the person from paragraph 1 of this Article. Within enhanced customer verification from paragraph 1 of this Article, in addition to identification from Article 7 of this Law, an reporting entity shall: 1. obtain data on funds and asset sources, that are the subject of a business relationship or transaction, from personal or other documents submitted by a customer, and if the prescribed data cannot be obtained from the submitted documents, the data shall be obtained directly from a customer's written statement; 2. obtain a written consent of the person in charge before establishing business relationship with a customer, and 3. after establishing a business relationship, monitor with special attention transactions and other business activities carried out with an institution by a politically exposed person. An reporting entity shall by an internal enactment, in accordance with the guidelines of a competent supervisory authority, determine the procedure of identifying a politically exposed person. Article 25 of the LPMLTF defines the Enhanced Customer Verification Enhanced customer verification, in addition to the identification from Article 7 of this Law, shall include additional measures in the following cases: 1. on entering into open account relationship with a bank or other similar credit institution, with registered office outside the EU or outside the states from the list; 2. on entering into business relationship or executing transaction from Article 9 paragraph 1 item 2 of this Law with a customer that is a politically exposed person from Article 27 of this Law, and 3. when a customer is not present during the verification process of establishing and verifying the identity. An reporting entity shall apply a measure or measures of enhanced customer verification from Articles 26, 27 or 28 of this Law in the cases when he/she/it estimates, that due to the nature of a business relationship, type and manner of transaction execution, business profile of a customer or other circumstances related to the customer, there is or there could be a risk of money laundering or terrorist financing. As the constituent part of the Guidelines about the risk analysis assessment in the scope of money laundering and terrorism financing assessment for reporting entities from the Article 4. Paragraph 2. items 14. and 15. of the LPMLTF, the APMLFT determined form for PEP identification. The reporting entity receives information whether the specific customer is politically exposed persons or not from specific written and signed notification which is given to

the customer to be fulfilled before concluding business relation or carrying out the transaction (Questionnaire for Identification of PEPs). Written notification needs to be drafted both in local and in English language).

QUESTIONNAIRE FOR IDENTIFYING A POLITICALLY EXPOSED PERSON

In accordance with the Law on the Prevention of Money Laundering and Terrorist Financing (hereinafter: the LPMLTF, Official Gazette of Montenegro, No. 14/07), ____________ (reporting entity) must establish whether a customer is a politically exposed person when entering into a business relationship or executing transactions (Article 9 Paragraph 1 Item 2) with the customer .

*A **politically exposed person** is any natural person who works or has worked in the last year in a high-profile public position, including that person's immediate family members and co-workers.*

***Immediate family members of a politically exposed person** are spouses or cohabiting partners, parents, brothers and sisters, as well as children and their spouses or cohabiting partners.*

***Immediate co-workers of a politically exposed person** are all persons who have joint income from property, an active business relationship or any other form of close business contact.*

Pursuant to the requirements of the LPMLTF, we are kindly requesting that you answer the following questions.

1. Are you:

1.	a head of state?	YES	NO
2.	the head of a government?	YES	NO
3.	a minister or deputy or assistant thereof?	YES	NO
4.	Head of state administrative body or local administrative body, or his /her deputy or assistant and other official?	YES	NO
5.	an elected representative of a legislative body (MPs and other person appointed or elected by the Parliament)	YES	NO
6.	a holder of the highest judicial and constitutional court functions (judges, prosecutors, and their deputies)	YES	NO
7.	a member of a court of auditors or supreme auditing institutions and central bank governing board?	YES	NO
8.	an ambassador?	YES	NO
9.	A consul? (diplomatic agents)?	YES	NO
10.	a high-ranking officer in the armed forces?	YES	NO
11.	a member of the management or supervisory board of a company under majority state ownership?	YES	NO

2. Are you:

1.	An immediate family member of the persons defined in point 1? • Spouse of cohabiting partner • Parent • Brother or sister • Child born in a marital or extramarital relationship and his or her spouse or cohabiting partner	 YES YES YES YES	 NO NO NO NO
2.	An immediate co-worker of the persons defined in point 1 • Do you have joint income from property or an active business relationship with the persons defined above? • Do you have any other form of close business contact with the persons defined above?	 YES YES	 NO NO

3. Have you:

In the last 12 months worked in any of the positions set out in point 1?	YES	NO
Are you an immediate family member or co-worker of a person who has worked in any of the positions, set out in point 1, in the last 12 months?	YES	NO

	If you have answered YES to any of the above questions, you are considered a politically exposed foreign person according to the law. We therefore kindly request that you state the origin of funds and property that are or will be the subject of the business relationship or transaction:
	I, the undersigned, hereby confirm that the above stated data are correct and true. _______________________________________ Name and surname of person completing the questionnaire Customer's address Customer's data of birth Place and date Signature of the customer
	_______________________________________ Name and surname of the bank employee Place and date Signature of the bank employee
	I hereby authorise the entering into a business relationship with a politically exposed person. _______________________________________ Name and surname of the responsible senior staff member Place and date Signature of the responsible senior staff member

“Tipping off”	
Please indicate whether the prohibition is limited to the transaction report or also covers ongoing ML or TF investigations.	**Prohibition of giving information** Article 80 of the LPMLTF determines: Reporting entities and reporting entity’s employees, members of authorised, supervising or managing bodies, or other persons, to which were available data from Article 71 of this Law, shall not reveal to a customer or third person: 1. that data, information or documentation on the customer or the transaction, from Article 33 paragraph 2, 3 and 4, Article 43 paragraph 1, Article 48 paragraph 1, 2 and 3, Article 49 paragraph 1 and 2 of this Law, are forwarded to the competent administration body ; 2. that the competent administration body on the basis of Article 51 of this Law, temporarily suspended transaction or in accordance with that gave instructions to the reporting entity; 3. that the competent administration body on the basis of Article 53 of this Law demanded regular supervision of customer’s financial business;

	4. that against customer or third party is initiated or should be initiated investigation for the suspicion of money laundering or terrorist financing . The information about the facts from paragraph 1 of this Article and notification on suspicious transactions or information about other offences from Articles 55 and 56 of this Law, are the official secret and designated as such, in accordance with Law. On removing the official secret designation, from paragraph 2 of this Article shall decide the authorised person of the administration. Prohibition of giving information from paragraph 1 of this Article shall not be applied on: 3. data, information and documentation, that are, in accordance with this Law obtained and kept by reporting entity, and necessary for establishing facts in criminal proceedings, and if submitting those data in written form is required or ordered by the Competent court, and 4. data from item 1 of this Article, if it is demanded by supervision body from Article 86 of this Law for the reasons of carrying out the provisions of this Law and regulations passed on the basis of this Law. **Disclosing a Business Secret is criminalized in the Article 280 of the Criminal Code (Official Gazette of the RM 70/03, 13/04, 47/06, and Official Gazette of the RM 40/08)** (1) Anyone who without authorisation communicates to another, hands over or in any other manner makes available data representing a business secret or who obtains such data with the intention to hand them over to an unauthorised person, shall be punished by an imprisonment sentence of three months to five years. (2) If the offence referred to in paragraph 1 of this Article was committed out of greed or with reference to strictly confidential data or in order to make the data public or use them abroad, the offender shall be punished by an imprisonment sentence from two to ten years. (3) Anyone who commits an offence referred to in paragraph 1 of this Article out of negligence, shall be punished by an imprisonment sentence not exceeding three years. (4) Business secrets are deemed to be data and documents which were proclaimed as such by means of a law, other regulation or decision of a competent authority passed under law, and whose disclosure would or could cause detrimental consequences for a business organisation or other business entity. Business secret is also determined in the Law on Civil Servants and State Employees Article 52 (Law on Civil Servants and State Employees (Official Gazette of Montenegro 50/08 and 86/09) states: *"A Civil Servant, i.e. State Employee shall keep an official secret stipulated by the law or other regulation, regardless of the manner in which he/she has learned about it.* *The obligation to keep an official secret shall last even after the termination of employment, but no longer than five years from the day of the termination of office. Exceptionally, the obligation to keep an official secret may last even longer, when this is stipulated by the law.* *The head of a state authority may release a Civil Servant, i.e. State Employee, from the obligation to keep an official secret during a court or administrative procedure, if it relates to data without which the establishment of facts and making of a legal decision would not be possible."* Article 59 of the same Law determines that the reviling of business, professional and other secret is determined by the Law and by other regulations and is a serious

	disciplinary offence: *Serious disciplinary offences are:* *- a fine in the amount of 20 to 30% of a salary paid in the month in which the offence was committed;* *- termination of employment.*
With respect to the prohibition of "tipping off" please indicate whether there are circumstances where the prohibition is lifted and, if so, the details of such circumstances.	As it is defined in the previous response On removing the official secret designation from Article 80, paragraph 2 of the LPMLTF shall decide the authorised person of the administration. Article 80 paragraph 4 defines: Prohibition of giving information from paragraph 1 of this Article may not be applied on: 1. data, information and documentation, that are, in accordance with this Law obtained and kept by reporting entity, and necessary for establishing facts in criminal proceedings, and if submitting those data in written form is required or ordered by the Competent court, and 2. data from item 1 of this Article, if it is demanded by supervision body from Article 86 of this Law for the reasons of carrying out the provisions of this Law and regulations passed on the basis of this Law.

"Corporate liability"	
Please indicate whether corporate liability can be applied where an infringement is committed for the benefit of that legal person by a person who occupies a leading position within that legal person.	This possibility exists. In accordance with the Law on Liability of Legal Entities for Criminal Offences ("Official Gazette of the Republic of Montenegro" 2/2007), a legal person liable for a criminal offence of the responsible person who acting on behalf of the legal person within its competence commits a criminal offence with the intent to acquire some gain for that legal person. The liability of the legal person exists also when the acting of that responsible person was contrary to the business politics or orders of the legal person. Regarding the limits of liability of a legal person for criminal acts, when the legal conditions are met, a legal person is liable for a criminal act even if the responsible person who committed the criminal act was not convicted for that criminal act. The law also stipulates that the liability of a legal person does not exclude criminal liability of the responsible person for the committed criminal act. In accordance with the provision Article 5 of the Law on Liability of Legal Persons for Criminal Offences ("Official Gazette of the Republic of Montenegro" 2/2007, 13/2007), a legal person can also be liable for a money laundering offence.
Can corporate liability be applied where the infringement is committed for the benefit of that legal person as a result of lack of supervision or control by persons who occupy a leading position within that legal person.	As above stated, a legal person is liable for the criminal offence of a responsible person who acting on behalf of the legal person within its competence commits a criminal offence with the intent to acquire some gain for that legal person**.** The Criminal Code of Montenegro stipulates that a criminal offence can be done by an act or omission (Article 6). Offence is done by omission when the perpetrator omitted the act which he/she was obliged to do. Also, an offence that is legally not determined as omission can be done by omission, if the perpetrator achieved characteristics of offence by omitting the due act. According to that, common liability can be applied when the act was committed to the benefit of legal person due to lack of supervision or control of the responsible person in the legal person.

DNFBPs	
Please specify whether the obligations apply to all natural and legal persons trading in all goods where payments are made in cash in an amount of € 15 000 or over.	Article 4 paragraph 2 of the LPMLTF: Measures from Paragraph 1 of this Article shall be undertaken by business organisations, other legal persons, entrepreneurs and natural persons (hereinafter referred to as: reporting entities), as follows: 1) banks and foreign banks' branches and other financial institutions; 2) savings-banks, and savings and loan institutions; 3) organisations performing payment transactions, 4) post offices, 5) companies for managing investment funds and branches of foreign companies for managing investment funds; 6) companies for managing pension funds and branches of foreign companies for managing pension funds; 7) stock brokers and branches of foreign stock brokers; 8) insurance companies and branches of foreign insurance companies dealing with life assurance; 9) organisers of lottery and special games of chance; 10) exchange offices; 11) pawnshops; 12) audit companies, independent auditor and legal or natural persons providing accounting and tax advice services; 13) institutions for issuing electronic money; 14) humanitarian, nongovernmental and other non-profit organisations, and 15) other business organisations, legal persons, entrepreneurs and natural persons engaged in an activity or business of: - sale and purchase of claims; - factoring; - third persons' property management; - issuing and performing operations with payment and credit cards; - financial leasing; - travel organisation; - real estate trade; - motor vehicles trade; - vessels and aircrafts trade; - safekeeping; - issuing warranties and other guarantees; - crediting and credit agencies; - granting loans and brokerage in loan negotiation affairs; - brokerage or representation in life insurance affairs, and - organising and conducting biddings, trading in works of art, precious metals and precious stones and precious metals and precious stones products, as well as other goods, when the payment is made in cash in the amount of € 15.000 or more, in one or more interconnected transactions.

6. Statistics

a. Please complete - to the fullest extent possible - the following tables:

2005												
	Investigations		**Prosecutions**		**Convictions (final)**		**Proceeds frozen**		**Proceeds seized**		**Proceeds confiscated**	
	cases	**persons**	**cases**	**persons**	**cases**	**persons**	**cases**	**amount** (in EUR)	**cases**	**amount** (in EUR)	**cases**	**amount** (in EUR)
ML	3	8	1	1	1	1						
FT												

2006												
	Investigations		**Prosecutions**		**Convictions (final)**		**Proceeds frozen**		**Proceeds seized**		**Proceeds confiscated**	
	cases	**persons**	**cases**	**persons**	**cases**	**persons**	**cases**	**amount** (in EUR)	**cases**	**amount** (in EUR)	**cases**	**amount** (in EUR)
ML	7	39	7	42	1	1				1958000€		161000€
FT												

2007												
	Investigations		**Prosecutions**		**Convictions (final)**		**Proceeds frozen**		**Proceeds seized**		**Proceeds confiscated**	
	cases	**persons**	**cases**	**persons**	**cases**	**persons**	**cases**	**amount** (in EUR)	**cases**	**amount** (in EUR)	**cases**	**amount** (in EUR)
ML	2	11	1	10								
FT												

2008												
	Investigations		**Prosecutions**		**Convictions (final)**		**Proceeds frozen**		**Proceeds seized**		**Proceeds confiscated**	
	cases	**persons**	**cases**	**persons**	**cases**	**persons**	**cases**	**amount** (in EUR)	**cases**	**amount** (in EUR)	**cases**	**amount** (in EUR)
ML	3	7	2	5	1	4				87600€		
FT												

2009												
	Investigations		**Prosecutions**		**Convictions (final)**		**Proceeds frozen**		**Proceeds seized**		**Proceeds confiscated**	
	cases	**persons**	**cases**	**persons**	**cases**	**persons**	**cases**	**amount** (in EUR)	**cases**	**amount** (in EUR)	**cases**	**amount** (in EUR)
ML												
FT												

SUPREME STATE PROSECUTOR'S OFFICE
Statistical data for the criminal offence- money laundering for the period from 2004 to 31.12.2009

Year	No. cases	No. persons	investigation		Temporary measures		Amount of proceeds derived from crime	Termination of investigation		Pending investigation		Raised indictment		Confiscation proposed	Convictions		Conviction based confiscation)	Transferred criminal cases	
			No. cases	No. persons	No. cases	No. persons		No. cases	No. persons	No. cases	No. persons	No. cases	No. persons		No. cases	No. persons		No. cases	No. persons
2004	2	3	1	2			895 000 $					1	2	895 000 $	1	2	895 000 $	1	1
2005	3	8	3	8			over 40 000 €	2	7			1	1		1*	1			
2006	10	53	7	39	4	31	5 965 000 €			2	8	7	42	1958000€	1* 1**	1* 2**	161 000€	1	3
2007	2	11					190 000€ ****					1	10					1	1
2008	3	7	3	7	1	1	over 80 000€			1	2	2	5	87.600€	1*	4*			

* Conviction of release.
** Conviction is not final.
**** In the case in which the investigation is being conducted was not suggested to determinate temporary measure, because this measure has already been determined against the same persons in the case from 2006

b. STR/CTR

Explanatory note:
The statistics under this section should provide an overview of the work of the FIU.
The list of entities under the heading "*monitoring entities*" is not intended to be exhaustive. If your jurisdiction covers more types of monitoring entities than are listed (e.g. dealers in real estate, supervisory authorities etc.), please add further rows to these tables. If some listed entities are not covered as monitoring entities, please also indicate this in the table.

The information requested under the heading "*Judicial proceedings*" refers to those cases which were initiated due to information from the FIU. It is not supposed to cover judicial cases where the FIU only contributed to cases which have been generated by other bodies, e.g. the police.

"C*ases opened*" refers only to those cases where an FIU does more than simply register a report or undertakes only an IT-based analysis. As this classification is not common in all countries, please clarify how the term "cases open" is understood in your jurisdiction (if this system is not used in your jurisdiction, please adapt the table to your country specific system).

2005																			
Statistical Information on reports received by the FIU								Judicial proceedings											
Monitoring entities, e.g.	reports about transactions above threshold	reports about suspicious transactions		cases opened by FIU		notifications to law enforcement/ prosecutors		indictments				convictions							
								ML		FT		ML		FT					
		ML	FT	ML	FT	ML	FT	cases	persons	cases	persons	cases	persons	cases	persons				
Commercial Banks		500																	
Insurance Companies	4																		
Notaries																			
Currency Exchange																			
Broker Companies	3.275																		
Securities' Registrars																			
Lawyers																			
Accountants/Auditors																			
Company Service Providers																			
Car dealers	393																		
Real estate agents	349																		
Organisers of games of chance	1																		
Total		500		158		**27**													

*** Cash transactions 20.755 +78.934*Cashless transactions = 99689 CTR**

Reports received from the competent state authorities

Customs	161	7	
Post office	4		
Stock exchange markets	110.042*		

CDA	663*		

2006															
Statistical Information on reports received by the FIU								Judicial proceedings							
Monitoring entities, e.g.	reports about transactions above threshold	reports about suspicious transactions		cases opened by FIU		notifications to law enforcement/ prosecutors		indictments				convictions			
								ML		FT		ML		FT	
		ML	FT	ML	FT	ML	FT	cases	persons	cases	persons	cases	persons	cases	persons
Commercial Banks	49.539 CTR	183													
Insurance Companies	1														
Notaries															
Currency Exchange															
Broker Companies	3	1													
Securities' Registrars															
Lawyers															
Accountants/ Auditors															
Company Service Providers															
Car dealers	234														
Real estate dealers	96														
Total		**184**		**286**		**29**									

***Cash transactions 41.140 +8.399*Cashless transactions = 49.539 Currency Transaction Reports**

Reports received from the competent state authorities

Customs	**218**	**2**	
Post office	**31**		
Stock exchange market	111.809		
CDA	1.085		

2007															
Statistical Information on reports received by the FIU								Judicial proceedings							
Monitoring entities, e.g.	reports about transactions above threshold	reports about suspicious transactions		cases opened by FIU		notifications to law enforcement/ prosecutors		indictments				convictions			
								ML		FT		ML		FT	
		ML	FT	ML	FT	ML	FT	cases	persons	cases	persons	cases	persons	cases	persons
Commercial Banks	Cash transactions 87.026 +646*	104													
Insurance Companies															
Notaries															
Currency Exchange															
Broker Companies															
Securities' Registrars															
Lawyers															
Accountants/Auditors															
Company Service Providers															
Car dealers	**211**														
Real estate agents	512														
Total		**104**		**220**		**43**									

*** Cash transactions 87.026 +646Cashless transactions= 87672 Currency Transaction Reports**

Reports received from the competent state authorities

Courts(contracts)**	14.457**		
Customs	333	**12**	
Post office	42		
Stock exchange market	215.403		
CDA	161.432		

****APMLTF possesses data base with verified copies of real estate sales contracts that are provided by courts**

2008															
Statistical Information on reports received by the FIU								**Judicial proceedings**							
Monitoring entities, e.g.	**reports about transactions above threshold**	**reports about suspicious transactions**		**cases opened by FIU**		**notifications to law enforcement/ prosecutors**		**indictments**				**convictions**			
								ML		**FT**		**ML**		**FT**	
		ML	**FT**	**ML**	**FT**	**ML**	**FT**	**cases**	**persons**	**cases**	**persons**	**cases**	**persons**	**cases**	**persons**
Commercial Banks	*58.014 CTR	41													
Insurance Companies															
Notaries															
Currency Exchange															
Broker Companies	3	3													
Securities' Registrars															
Lawyers															
Accountants/Auditors															
Company Service Providers															
Car dealers	**199**														
Regal estate agents	338														
Organisers of games of chance	5														
		44		**148**		**38**									

*** Cash transactions 57.675 +339 Cashless transactions =58.014 Currency Transaction Reports**

Reports received from the competent state authorities

Courts (contracts)	8.887**		
Customs	387	**13**	
Post office	26		
Stock exchange markets	62.672		
CDA	79.859		

****APMLTF possesses data base with verified copies of real estate sales contracts that are provided by courts**

2009																			
Statistical Information on reports received by the FIU								**Judicial proceedings**											
Monitoring entities, e.g.	**reports about transactions above threshold**	**reports about suspicious transactions**		**cases opened by FIU**		**notifications to law enforcement/ prosecutors**		**indictments**				**convictions**							
								ML		**FT**		**ML**		**FT**					
		ML	**FT**	**ML**	**FT**	**ML**	**FT**	**cases**	**persons**	**cases**	**persons**	**cases**	**persons**	**cases**	**persons**				
Commercial Banks	*34.743 CTR	48																	
Insurance Companies																			
Notaries																			
Currency Exchange																			
Broker Companies	7																		
Securities' Registrars		2																	
Lawyers		1																	
Accountants/Auditors																			
Company Service Providers																			
Car dealers	**196**																		
Real-estate agents	**356**	**1**																	
Organisers of games of chance	192																		
Total		**52**		**269**		**130**													

*** Cash transactions 34.702 +41*Cashless transaction =34.743 Currency Transaction Reports**

Reports received from the competent state authorities

Courts (contracts)**	3.888**		
CDA	53.663		
Customs	344	**38**	
Post office	5		
Stock exchange markets	33,262		
Department of Public Revenues		**1**	
Capital City Podgorica		**1**	
Analytics Department		**91**	
Anonymous tips			

****APMLTF possesses data base with verified copies of real estate sales contracts that are provided by courts**

APPENDIX I - Recommended Action Plan to Improve the AML / CFT System

AML/CFT System	**Recommended Action (listed in order of priority)**
1. General	**No text required**
2. Legal System and Related Institutional Measures	
2.1 Criminalisation of Money Laundering (R.1 & 2)	• The money laundering offence as defined by the Criminal Code is basically sound, but it lacks further refinement; the current formulation of criminalised behavior (conversion/transfer and concealment/disguise) is narrower than the requirements in the Vienna and Palermo Conventions and should be clarified in the Criminal Code. • The Criminal Code should be amended to clearly include insider trading and market manipulation offences as predicate offences for money laundering. • There is relatively strict regulation of extraterritoriality in the case of offences committed by persons who are not citizens of Montenegro against a foreign state. This also raises the question of inclusion of "all serious offences" in the predicate offences. This is subject to incriminations in those countries and if offences are not punishable with at least 5 years imprisonment, the offence would not be considered a predicate offence in Montenegro. Abolition of this limitation (5 years imprisonment) would prevent such situations.
2.2 Criminalisation of Terrorist Financing (SR.II)	• A definition of "funds", which includes "assets of every kind, whether tangible or intangible, movable or immovable, however, acquired, and legal documents or instruments in any form, including electronic or digital, evidencing title to, or interest in, such assets, including, but not limited to, bank credits, travellers cheques, bank cheques, money orders, shares, securities, bonds, drafts, letters of credit." should be laid down in the Criminal Code. • The reference to specific criminal offences (terrorism, international terrorism and hostage taking) in Article 449 should be brought into line with the scope of the Terrorist Financing Convention and the Interpretive Note to SR II, as the scope which constitutes the criminal offence becomes narrower. Under Articles 365 and 447, only the acts, intended to *cause harm* (to the constitutional order of Montenegro, or the foreign state/international organisation) are criminalised, while the convention requires the incrimination of any acts of violence which purpose is to *intimidate* a population or *compel* a government or international institution (to

	do/to abstain from doing). • The Criminal Code should be amended to incorporate the incrimination of funding of terrorist organisations and individual terrorists. • The solution of relating the existence of the terrorist financing offence to specific criminal offences, found under other Articles of the CC is also appropriate (IN 6). Under current legislation, terrorist financing is only considered to be a criminal offence if funds are intended for one of three specific criminal offences (Terrorism, Article 365, International Terrorism, Article 447 and Hostage Taking, Article 448). A more flexible definition which would incriminate financing. Furthermore, there needs to be an offence introduced to cover cases when funds are not linked with a specific terrorist. • Article 449 of the Criminal Code should be brought into line with international standards.
2.3 Confiscation, freezing and seizing of proceeds of crime (R.3)	• The Criminal Code should be amended to give a more comprehensive definition of "organised crime". • A reversal of the burden of proof regarding property subject to confiscation should be introduced. • A legal authority should be established to take steps to prevent or void actions where the person involved knew or should have known that the authorities would be prejudiced in their ability to recover property subject to confiscation
2.4 Freezing of funds used for terrorist financing (SR.III)	• A central authority at national level to examine, integrate and update the received lists of persons and entities suspected to be linked to international terrorism before sending them to the financial sector and DNFBP should be introduced. • A domestic mechanism to enact S/RES/1373 (2001) should be implemented to be able to designate terrorists at national level as well as to give effect to designations and requests for freezing assets from other countries. • Procedures for evaluating de-listing requests, for releasing funds or other assets of persons or entities erroneously subject to the freezing and for authorising resources pursuant to S/RES/1452 (2002) should be adopted. • Practical guidance to the financial institutions and DNFBP concerning their responsibilities under the freezing regime as well as for the reporting of suspicious transactions that may be linked to terrorism financing should be issued by the authorities.
2.5 The Financial Intelligence Unit and its functions (R.26)	• Specific criteria should be developed indicating the competent authority to receive the notification from APMLTF which normally starts an investigation. • APMLTF should take into consideration the necessity of expanding their direct access to other authorities'

	databases. • An updated List of Suspicious Transactions Indicators should be issued and regularly updated. • a register on reporting entities to be supervised by APMLTF should be maintained. • APMLTF should be staffed sufficiently to supervise the very large number of reporting entities. • The prohibition for the dissemination of information received by APMLTF's employees, after cessation of working, should be an explicit provision in the law without any time limit.
2.6 Law enforcement, prosecution and other competent authorities (R.27 & 28)	• The Prosecution Authority should implement a rigorous supervision mechanism in order to avoid unnecessarily returning cases to Police Administration, which may lead to a negative impact on the effectiveness of the system. • The special investigative techniques should be extended to all forms of money laundering to enable law enforcement authorities to ensure a proper investigation. • All law enforcement authorities should continue to strengthen inter-agency AML/CFT training programmes in order to have specialised financial investigators and experts at their disposal. • Further steps need to be taken to eradicate the perception of corruption in law enforcement bodies.
2.7 Cross Border Declaration & Disclosure	• The Customs Administration should be given clear powers to stop individuals and restrain currency in all circumstances. • The Customs Administration should have the legal authority to restrain currency in cases of an administrative offence. • The Customs Administration should take into consideration a system to use reports on currency declaration in order to identify money launderers and terrorists. • The administrative sanctions for false declarations or non-declared currency should be raised considerably. Taking into account the low chance of detection, the fines are not considered to be dissuasive or effective. • In order to increase its effectiveness, the Customs Administration should hire more specialised staff to deal with money laundering and terrorist financing cross-border transportation of currency.
3. Preventive Measures – Financial Institutions	
Risk of money laundering or terrorist financing	
3.2 Customer due diligence,	• It is the view of the evaluators that the wording of the second point under Article 9 is too precise and could be

including enhanced or reduced measures (R.5 to 8)	interpreted to read that only transactions of exactly €15,000 require CDD. The evaluators consider that**”or more”** should be added in Article 9, Paragraph 1 number 2 in the LPMLTF. • The LPMLTF should be amended to require CDD to be conducted on wire transactions of €1,000 or more. • The LPMLTF should be amended to require obligors to verify that persons purporting to act on behalf of a customer have the authority to act on behalf of the customer. Article 15 of the LPMLTF should be amended to require the obtaining of copies of the document regulating the power to bind the legal person or arrangement. • The problem of reliance on certificates from the commercial register for CDD purposes should be addressed by establishing procedures to address the limitations of the commercial register. • Article 29.4 of the LPMLTF appears to go further than intended by Criteria 5.9 in that it permits simplified customer verification in respect of customers to “whom an insignificant risk of money laundering or terrorist financing is related” which could include a broader range of customers than those envisaged in Criteria 5.9. Article 29.4 should be amended to bring it into line with the essential criteria. • The FATF definition (“*Beneficial owner* refers to the natural person(s) who ultimately owns or controls a customer and/or the person on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate effective control over a legal person or arrangement.”) should be incorporated into the LPMLTF and a requirement to identify and verify the “ultimate” beneficial owner should be included. • Article 25 of the LPMLTF is very specific and does not cover a number of the specified categories as set out in Criteria 5.8, namely all non-resident customers, private banking, legal persons or arrangements such as trusts that are personal assets holding vehicles and companies that have nominee shareholders or shares in bearer form. The evaluators consider that the LPMLTF should be amended to fully reflect all of the categories in Criteria 5.8. • Risk guidelines in accordance with Criteria 5.12 should be completed and published. • A specific clause should be inserted into the LPMLTF requiring obligors to consider making a suspicious transaction report in circumstances where they have been unable to conduct satisfactory CDD. Likewise there should also be a clause requiring obligors to

	terminate a business relationship in circumstances where they have been unable to conduct satisfactory CDD. This is particularly relevant in circumstances where CDD has not been possible for existing customers where there are one or more linked transactions amounting to €15,000, etc.. • There needs to be a specific requirement for obligors to assess and consider the risks of technological developments as part of their risk analysis. This should also be introduced in the guidelines to be produced by the supervisory bodies. • It is the view of the evaluators that the requirements of Criteria 5.17 are essentially met although the wording of the first point above is too precise and could be interpreted to read that only transactions of exactly €15,000 require CDD. Furthermore, the requirement is for CDD to be conducted when "a transaction of significance takes place." and in the context of Criteria 5.17 it is considered that this is more appropriate wording. Overall the evaluators consider that a separate clause should be inserted into the LPMLTF to specifically deal with the issue of CDD on existing customers. • The lack of awareness as regards PEPS and the consequent lack of proper procedures to address the risk should be addressed through proper training to be followed by the establishment of adequate procedures to address this risk. • Article 25 of the LPMLTF should be amended to extend the requirement to all cross-border correspondent banking and other similar relationships. • A requirement for financial institutions to have policies and procedures to address the risk of misuse of technological developments in ML/TF schemes should be introduced. • Regulations should clearly establish the obligation to obtain information on the purpose and intended nature of the business relationship for non-face to face business.
3.3 Third parties and introduced business (R.9)	• The Montenegrin authorities should consider amending legislation to specifically prohibit financial institutions from relying on intermediaries or other third parties to perform specified elements of the CDD process.
3.4 Financial institution secrecy or confidentiality (R.4)	
3.5 Record keeping and wire transfer rules (R.10 & SR.VII)	• There is no requirement that transaction records should be sufficient to permit reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of criminal activity in accordance with the requirements of essential criteria 10.1.1. The LPMLTF should be amended to take this requirement into

	account. • The requirements of Special Recommendation VII should be incorporated into the legislation of Montenegro.
3.6 Monitoring of transactions and relationships (R.11 & 21)	• Financial institutions should be required to examine as far as possible the background and purpose of unusual transactions. Enforceable requirements to set forth the finding of such examinations in writing should equally be provided. In addition specific enforceable requirement should be put in place for financial institutions to keep such findings available for authorities and auditors for at least five years. • Financial institutions should be required to give special attention to business relationships and transactions with persons from or in countries which do not or insufficiently apply the FATF recommendations. Effective measures should be put in place to ensure that financial institutions are advised of concerns about weaknesses in the AML/CFT systems of other countries and consideration should be given to the development of appropriate countermeasures as set out in the essential criteria to Recommendation 21.
3.7 Suspicious transaction reports and other reporting (R.13-14, 19, 25 & SR.IV)	• The reporting obligation should be extended to include money laundering reporting obligations if the transaction has already been performed. • The Book of Rules, should be endorsed in law with sanctions for breaches in order to become “other enforceable means”. • A provision should be introduced to ensure that the names and personal details of staff of financial institutions that make a STR are kept confidential by APMLTF. • APMLTF should provide regular general feedback to all obligors which should contain: (a) statistics on the number of disclosures, with appropriate breakdowns, and on the results of the disclosures; (b) information on current techniques, methods and trends (typologies); and (c) sanitised examples of actual money laundering cases.
3.8 Internal controls, compliance, audit and foreign branches (R.15 & 22)	• Requirements should be developed that require financial institutions to put in place screening procedures to ensure high standards when hiring employees. • The inspection procedures that have been introduced by the Central Bank should be adopted by other financial services supervisors.
3.9 Shell banks (R.18)	
3.10 The supervisory and	• Although APMLTF provides general information on

oversight system - competent authorities and SROs. Role, functions, duties and powers (including sanctions) (R.23, 29, 17 & 25)	criteria for detection of suspicious activity as required in the LPMLTF guidelines referring to specific AML/CFT risk factors and measures to mitigate such risks should also be provided. • Typologies should be developed and presented to reporting entities. • There is a need to provide more guidance on AML/CFT issues, with particular focus on the non-banking sector.
3.11 Money value transfer services (SR.VI)	• The requirements of Special Recommendation VI need to be implemented. • The Montenegrin authorities should introduce legislation to enforce the licensing/registration of all MVT service providers together with appropriate sanctions.
4. Preventive Measures – Non-Financial Businesses and Professions	
4.1 Customer due diligence and record-keeping (R.12)	• Trust and Company Service Providers should be designated as obliged parties. • For casinos, CDD should be required above the €3,000 threshold. • There should be a clear requirement for casinos to link the incoming customers to individual transactions. • Effective systems for monitoring and ensuring compliance with CDD requirements across most of the DNFBP sectors need to be developed. • DNFBPs need to be made aware of their obligations regarding PEPs. Specific guidelines, aimed at DNFBPs should be developed. It is also recommended that a training programme be undertaken concerning the risks and controls necessary concerning dealings with politically exposed persons. • A requirement should be introduced for DNFBPs to have policies in place to prevent the misuse of technological developments in ML/TF. • More attention need to be given to raising awareness and enforcing compliance in casinos
4.2 Suspicious transaction reporting (R.16)	• The obligation to report suspicious transactions that have been performed should be explicitly provided for in either law or regulation. • A prohibition against tipping off should be made specifically applicable to lawyers. • More targeted training to sectors that pose the greatest risk should be considered.
4.3 Regulation, supervision and monitoring (R.24-25)	• A comprehensive register of all reporting entities should be developed by APMLTF. • Guidelines to assist DNFBPs in implementing and complying with respective AML/CFT requirements are, at should be developed. Adequate and appropriate feedback on suspicious transaction reporting for

	DNFBPs should be provided.
4.4 Other non-financial businesses and professions (R.20)	• Montenegro has extended its AML/CFT obligations to other non-financial businesses, however, a regulatory and supervisory framework needs to be developed to ensure that FATF Recommendations 5, 6, 8 to 11, 13 to 15, 17 and 21 are being adhered to by these non-financial businesses. • A risk analysis to determine which other non-financial businesses and professions are at greatest risk of being misused for money laundering and/or terrorist financing should be undertaken. Based upon the results of such analysis, the authorities of Montenegro should direct priority outreach and educational efforts to those other non-financial businesses at the highest levels of risk.
5. Legal Persons and Arrangements & Non-Profit Organisations	
5.1 Legal Persons – Access to beneficial ownership and control information (R.33)	• The acquisition of information on beneficial owners by the agencies and institutions which deal with clients form abroad seems to be less effective. Considering the very intensive involvement of foreign legal entities on the Montenegrin real-estate market and rather poor information on beneficial ownership in such entities, this might present a considerable risk of abuse of such legal entities for money laundering and terrorist financing and it is recommended that financial institutions and DNFBPs be reminded to apply the same standards to overseas customers as to domestic. • Consideration should be given to the risk of foreign bearer shares being sold in Montenegro.
5.2 Legal Arrangements – Access to beneficial ownership and control information (R.34)	
5.3 Non-profit organisations (SR.VIII)	• Montenegro should conduct a review of the adequacy of its legal framework that relates to NPOs that can be abused for terrorism financing. • Montenegro should implement measures to ensure that terrorist organisations cannot pose as legitimate NPOs. • Montenegro should also reach out to the NPO sector with a view to protecting the sector from terrorist financing abuse. This outreach should include i) raising awareness in the NPO sector about the risks of terrorist abuse and the available measures to protect against such abuse; and ii) promoting transparency, accountability, integrity, and public confidence in the administration and management of all NPOs. • Montenegro should take more proactive steps to promote effective supervision or monitoring of NPOs. Authorities should ensure that detailed information on

	the administration and management of NPOs are available during the course of an investigation or on request internationally. Montenegro should also implement effective sanctions for violations of oversight measures or rules by NPOs or persons acting on behalf of NPOs.
6. National and International Co-operation	
6.1 National co-operation and coordination (R.31)	• Formal arrangements for co-operation between policy makers, FIU, law enforcement and supervisory bodies at a strategic level for AML/CFT should be developed. • At the operational level, the evaluators recommend that additional formal agreements be concluded in order to define the type of information to be exchanged, timeliness of the exchange, the names of contact person, etc.. The Montenegrin authorities should aim to continue interdepartmental coordination and to release periodically analysis which will enable them to develop and implement policies and activities to combat money laundering and terrorist financing at a national level. • The evaluators recommend that the Montenegrin authorities review periodically the performance of the system as a whole against some key strategic performance indicators and review, collectively, as much as possible, the available statistical information to better carry out each agency's task and enhance AML/CFT framework.
6.2 The Conventions and UN Special Resolutions (R.35 & SR.I)	• As was already stated under 2.1 above, the incrimination of money laundering is limited to actions, defined as "business operations", which is narrower than the convention and this formulation should be further refined. • Laws and mechanisms for immediate freezing of the funds belonging to or intended for the designated terrorist organisations or individuals as defined by Resolution S/RES/1267 (1999) should be put in place.
6.3 Mutual Legal Assistance (R.36-38 & SR.V)	• With regard to financing of terrorism there are more problems present. Besides the narrower definitions of the financing of terrorism offence, the main shortcoming is inadequate implementation of UN Resolutions, primarily S/RES/1267 (1999). Regarding the incrimination of terrorist financing, the most important outstanding issues are: existing limitation of criminalisation on financing to concrete terrorist offences and, linked to that, inability of the present definition of criminal offence to also include the funds intentioned for terrorist organisations or individual terrorists.

	• Laws and mechanisms for immediate freezing of the funds belonging to or intended for the designated terrorist organisations or individuals as defined by Resolution S/RES/1267 (1999) should be put in place. • An asset forfeiture fund should be established.
6.4 Extradition (R.39, 37 & SR.V)	
6.5 Other Forms of Co-operation (R.40 & SR.V)	
7. Other Issues	
7.1 Resources and statistics (R. 30 & 32)	• APMLTF needs to enhance the training for its own staff and for reporting entities, in order to increase the awareness and understanding of money laundering and terrorism financing schemes which may be used • There is a need ensure that an international training programme on money laundering and terrorism financing issues is created and implemented. • The evaluators were concerned that there were not sufficient staff in APMLTF to supervise the very large number of reporting entities and recommend that the staff level be raised. • Clear comprehensive and well-structured statistics should be kept systematically. Such statistics should differentiate the amounts of assets, types of measures, duration of measures and primarily request/imposition ratio, etc.. These statistics should then be utilised to measure the effectiveness of the system of confiscation, freezing and seizing of proceeds of crime.
7.2 Other relevant AML/CFT measures or issues	
7.3 General framework – structural issues	

APPENDIX II

Excerpt from Directive 2005/60/EC of the European Parliament and of the Council, formally adopted 20 September 2005, on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing

Article 3 (6) of EU AML/CFT Directive 2005/60/EC (3rd Directive):

(6) "beneficial owner" means the natural person(s) who ultimately owns or controls the customer and/or the natural person on whose behalf a transaction or activity is being conducted. The beneficial owner shall at least include:
(a) in the case of corporate entities:
(i) the natural person(s) who ultimately owns or controls a legal entity through direct or indirect ownership or control over a sufficient percentage of the shares or voting rights in that legal entity, including through bearer share holdings, other than a company listed on a regulated market that is subject to disclosure requirements consistent with Community legislation or subject to equivalent international standards; a percentage of 25 % plus one share shall be deemed sufficient to meet this criterion;
(ii) the natural person(s) who otherwise exercises control over the management of a legal entity:
(b) in the case of legal entities, such as foundations, and legal arrangements, such as trusts, which administer and distribute funds:
(i) where the future beneficiaries have already been determined, the natural person(s) who is the beneficiary of 25 % or more of the property of a legal arrangement or entity;
(ii) where the individuals that benefit from the legal arrangement or entity have yet to be determined, the class of persons in whose main interest the legal arrangement or entity is set up or operates;
(iii) the natural person(s) who exercises control over 25 % or more of the property of a legal arrangement or entity;

Article 3 (8) of the EU AML/CFT Directive 2005/60EC (3rd Directive):

(8) "politically exposed persons" means natural persons who are or have been entrusted with prominent public functions and immediate family members, or persons known to be close associates, of such persons;
Excerpt from Commission directive 2006/70/EC of 1 August 2006 laying down implementing measures for Directive 2005/60/EC of the European Parliament and of the Council as regards the definition of ‘politically exposed person’ and the technical criteria for simplified customer due diligence procedures and for exemption on grounds of a financial activity conducted on an occasional or very limited basis.

Article 2 of Commission Directive 2006/70/EC (Implementation Directive):
Politically exposed persons

1. For the purposes of Article 3(8) of Directive 2005/60/EC, "natural persons who are or have been entrusted with prominent public functions" shall include the following:
(a) heads of State, heads of government, ministers and deputy or assistant ministers;
(b) members of parliaments;
(c) members of supreme courts, of constitutional courts or of other high-level judicial bodies whose decisions are not subject to further appeal, except in exceptional circumstances;
(d) members of courts of auditors or of the boards of central banks;
(e) ambassadors, chargés d'affaires and high-ranking officers in the armed forces;
(f) members of the administrative, management or supervisory bodies of State-owned enterprises.

None of the categories set out in points (a) to (f) of the first subparagraph shall be understood as covering middle ranking or more junior officials.
The categories set out in points (a) to (e) of the first subparagraph shall, where applicable, include positions at Community and international level.
2. For the purposes of Article 3(8) of Directive 2005/60/EC, "immediate family members" shall include the following:
(a) the spouse;
(b) any partner considered by national law as equivalent to the spouse;
(c) the children and their spouses or partners;
(d) the parents.
3. For the purposes of Article 3(8) of Directive 2005/60/EC, "persons known to be close associates" shall include the following:
(a) any natural person who is known to have joint beneficial ownership of legal entities or legal arrangements, or any other close business relations, with a person referred to in paragraph 1;
(b) any natural person who has sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the benefit de facto of the person referred to in paragraph 1.
4. Without prejudice to the application, on a risk-sensitive basis, of enhanced customer due diligence measures, where a person has ceased to be entrusted with a prominent public function within the meaning of paragraph 1 of this Article for a period of at least one year, institutions and persons referred to in Article 2(1) of Directive 2005/60/EC shall not be obliged to consider such a person as politically exposed.

APPENDIX III. ADDITIONAL INFORMATION

1. STATISTICS

The Central Bank conducted a total of 32 bank examinations in 2006, 2007, 2008 and 2009, as presented in the table below:

ON-SITE BANK EXAMINATIONS CONDUCTED IN

2006, 2007, 2008 and 2009

1.		2006	2007	2008	2009	Total
2.	Number of examinations	9	9	6	8	32

Bank reports	CBM - Types of violations and actions taken** in 2006, 2007, 2008 and 2009							
	2006	No. of violations	2007	No. of violations	2008	No. of violations	2009	No. of violations
Commercial Banks	- Article 9, paragraph 1 of Law on the Prevention of Money Laundering and Terrorist Financing (hereafter: LPMLTF) / **identification of the client: legal persons/.** - Article 14 paragraph 1 of LPMLTF, / **submission of reports to the Administration for the Prevention of Money Laundering in the prescribed timeframe/.** - Article 43 paragraph 1 (points 1, 2, 4 and 12) of LPMLTF / **identification: authorised person, clients, origin of money, code of activity and reasons for account opening/.** - Article 5 of the Rulebook on the manner of work of the authorised person, the manner of performing internal controls, keeping and protection of data, manner of keeping records and staff training (hereinafter: the Rulebook),/ **duties and responsibilities of authorised person for dealing with gathered information/.** **-** Article 6 of the Rulebook **/verification and testing of implementation of the Programme against money laundering and terrorist financing/.** - Article 16 of the Rulebook / **records of persons reviewing information and data/.**	2 2 4 2 3 1	- Article 9 paragraphs 1 and 5 of LPMLTF / **identification of clients: legal and natural persons – non-residents/.** - Article 11 paragraph 2 of LPMLTF / **annual renewal of documentation for legal persons – non-residents/.** - Article 43 paragraph 1 (points 1, 2, 3, 4, 12 and 14) of LPMLTF / **identification: authorised person, clients, origin of money, code of activity and reasons for account opening, ownership structure/.** - Article 6 of the Rulebook / **verification and testing of implementation of the Programme against money laundering and terrorist financing /.** - Article 7 of the Rulebook, **/annual report on the prevention of money laundering and terrorist financing /.** - Article 12 of the Rulebook / **keeping and protection of data, information and documents for which there is a reason for suspicion in money laundering and terrorist financing /.** - Article 16 of the Rulebook / **records of persons reviewing information and data /.**	4 1 4 4 2 1 2 1	- Article 5 of LPMLTF, with respect to Article 43 of LPMLTF / **identification of clients: / *** - Article 9 paragraph 1 with respect to Article 43 of LPMLTF / **identification of clients: legal persons /*** - Article 14 of LPMLTF, with respect to Article 71 of LPMLTF / **identification of clients: natural persons – non-residents /.** - Article 15 of LPMLTF, with respect to Article 71 of LPMLTF / **identification of clients: legal persons – non-residents /.** - Article 17 of LPMLTF, with respect to Article 71 of LPMLTF / **identification of clients: authorised persons /.**	1 1 3 2 2	**-**Article 14 of LPMLTF: **establishing and verifying a natural person identity – invalid public identification document** **-** Article 15 of LPMLTF **establishing and verifying the identity of a legal person, statement form the Commercial Court Registry – older than three months**; - Article 22 of LPMLTF: **monitoring business activities** **-** Article 23 of LPMLTF: **Repeated annual control of a foreign legal person;** **-** Article 38 of LPMLTF: **the Bank has not provided authorised person with adequate working conditions;** -Article 71 of LPMLTF: **identification of natural person, (data on activity – employment.**	1 1 1 1 1 2

***Note:** The examination of one bank commenced in 2007 was completed in 2008, therefore it is shown in the column for 2008.

****Note:** The procedure of imposing measures against banks is prescribed by the Banking Law (OGM 17/08). Provisions of Article 116 of the Banking Law, prescribes that if the Central Bank determines that specific bank has violated regulations it may undertake one of the following measures:

- Warn the bank in writing;
- conclude a written agreement with the bank making the bank bound to remove the irregularities found within a specified time;
- issue an **order** imposing one or more measures prescribed by this law;
- revoke the bank's license.

When the Central Bank undertakes the measures in the form of **order** as defined in more details in Article 118 of the Banking Law, it determines **in the order the amount of funds** that the bank will be bound to pay to the Deposit Protection Fund on account of additional depositor protection from consequences of possible bankruptcy or liquidation procedure that may be instituted in the bank, given that such amount may range from 0.1% to 1% of bank's own funds.

Pursuant to Article 91 of the Law on the Prevention of Money Laundering and Terrorist Financing (OGM 14/07 and 04/08), actions of first instance misdemeanour procedure, within jurisdiction of competent administrative body, performs authorised official for proceeding misdemeanour procedure, in accordance with Law.

The statistics of the APMLTF Misdemeanor Procedure Department

Cases opened and solved at the Misdemeanor Procedure Department from 17th November 2008 to 31st December 2008	
Number of cases received in 2008	**14**
Total number of solved cases	**6**
Number of cases where the fine was imposed	5
Number of cases where the cases were rejected	1
Number of current cases	**8**
Total amount of fines imposed	**13,860.00**
Total amount of trial procedure expenses	**300.00**

Cases opened and solved at the Misdemeanor Procedure Department from January 2009 to 31st December 200	
Number of unclosed cases from 2008	**8**
Total number of cases received in 2009	**29**
number of cases received from Reporting Entities Control Department	23
number of cases received from Analytics Department	4
number of cases received from Suspicious transactions department	2
Total number of current cases in procedure	**37**
Total number of solved cases	27
Number of cases where the fine was imposed	17
Number of cases where the warning was issued	2
Number of cases where the cases were rejected	5
Number of cases where the cases were resigned	3
Total number of current cases in procedure	**10**
Total amount of fines imposed	**51,180.00**
Total amount of trial procedure expenses	**1,380.00**
Total number of first instance final decisions	22
Total number of trial procedure expenses	15
Total amount of charged fines and trial procedure expenses	**40,929.10**
Submitted complaints	**8**
Confirmed decisions	6
Reversed decisions	1
Number of opened cases at misdemeanor council	1

Statistics of the APMLTF's Reporting Entities Control Department

The Reporting Entities Control Department has been established in accordance to the new LPMLTF and the new systematization and job positions organisation act, with a view to ensuring consistent implementation of the LPMLTF by reporting entities. The measures undertaken by this Department are regulated, besides the LPMLTF as the basic Law, by the Law on Supervision and Law on Misdemeanors.

In 2009 the Reporting Entities Control Department has achieved the following results:
- Carried out controls 166
- 23 requests for initiating a misdemeanor procedure against reporting entities were filed
- 22 notifications were delivered to the other state authorities, in the context of Art. 56 of the LPMLTF **(to Department of Public Revenues – 14 and Police Directorate – 8)**

The supervised reporting entities given by the business activities they carry out

Type of business activities	Conducted controls
Real estate agencies	67
Constructing companies	55
NGOs	11
Mediation in machines, ships, planes sales	10
Maritime traffic services	6
Other activities	17
Total	**166**

REPORT ON THE WORK OF THE INTERNATIONAL AND NATIONAL CO-OPERATION DEPARTMENT

01.01.2009 – 31.12.2009

In the above stated period, **295** data delivery requests and responses were processed, as follows:

- **107 data delivery requests - sent** to other countries, and these refer to 124 natural persons and 108 legal persons
- **91 responses** (to our data delivery requests) **– received** from other states, and these refer to 100 natural and 82 legal persons
- **51 data delivery requests – received,** and these refer to 313 natural persons and 134 legal persons
- **46 responses** to data delivery requests **sent** to other countries, referring to 203 natural persons and 164 legal persons
- **Obtained - 8 consents** for forwarding the received information;
- **Given- 16 consents** for forwarding the received information**.**

2. RULES ON CONDUCT OF BUSINESS OF LICENSED PARTICIPANTS AT THE CAPITAL MARKET

(Official Gazette of Montenegro, No.78/09)

Article 22

(6) The client submitting orders via phone, fax or some electronic means of communication may submit it upon identification with the personal identification password that authorised market participant is providing to the client upon signing the contract. The client is obliged to keep provided identification password as a confidential and must not make it available to the third persons.

(7) The licensed market participant is obliged to check identity of the client through the identification password that is contained in each service contract prescribing possibility of submitting orders through the fax, electronic means of communication or some other means not including the direct attendance of the client.

(8) When contracting delivery of orders via electronic means of communication, the licensed market participant is obliged to ensure:

- secure methods of client identification,
- all important elements of the contract to the stated in electronic message;
- registry of acceptance of orders at e-mail address and of its entering into book of orders;
- reply to the orders accepted within which the original message is noticeable;

(9) When contracting delivery of orders via telephone, fax or via electronic means, the licensed market participant reserves the right to, if the order is not clarified and/or is ambiguous, reject execution of the submitted order and has to inform the client in the manner of submitting such order.

3. INSTRUCTION ON RISK ANALYSIS OF MONEY LAUNDERING, „KNOW YOUR CLIENT" PROCEDURES AND OTHER PROCEDURES FOR RECOGNISING SUSPICIOUS TRANSACTIONS

Pursuant to article 8 paragraph 3 of the Law on the prevention of money laundering and terrorist financing (Official Gazette, no 14/7 and 4/08)**-** (hereinafter: Law), performing authority prescribed by the article 86 of the law**,** and related to the article 8 of the Rules on the work of authorised person, a way of conducting internal control, keeping and protecting data, manner of keeping registers and educating employees ("Official gazette of Montenegro", No. 55/05), Securities and Exchange Commission, on 91st session on November 11th, 2008 adopted

Article 1.

This instruction establishes detailed requirements for adopting procedures of authorised market participants at the capital market, investment and pension fund management companies and investment funds, custody banks and other persons who perform securities business as their professional activity (hereinafter: capital market participants), related to recognition of suspicious transactions at the capital market.

Article 2.

Participants at the capital market are obliged to establish risks factors upon which shall determine acceptability of the clients, especially based at the following facts:

c) Home country of the client, home country of the majority founder, and/or real owner of the client regardless of the position of such country on the list of non-cooperative countries and territories issued by the international body for control and combating of money laundering, on a list of countries presented as off-shore zones or uncooperative jurisdiction or on list states which participant on securities market considers risky upon its own estimations.

d) Home country of the person who conducts transactions with the client, regardless of the position of such a country at the lists from the item a) above;
e) Client, majority owner, and/or owners of the client against whom enforcement measures have been instituted in order to establish international peace and safety, in accordance with the Resolution of the United Nations Security Council;
f) unknown or unclear source of client's assets, or assets whose source client may not prove;
g) Cases in which it is doubtful that client is acting on his own behalf, or that he acts under orders of guidelines of the third party;
h) Uncommon performance of transaction, especially taking into the account its basis, amount and way of realisation, purpose of account opening and client's business – if the client is the person who performs business activity;
i) Cases when there are indices that client performs suspicious transactions;
j) Client is politically exposed person;
k) Accounts of other persons related to client;
l) Peculiarity of client's business;

Article 3.

Capital market participants establish acceptability of the client depending on a risk factors from the article 2 of this Instruction and may refuse to conclude a contract with the customer in relation to whom some of the abovementioned risk factors are established, or concluding or terminating of the already concluded contract condition upon fulfillment of some specific requirements prescribed by the general act of the capital market participant.

To establish if customer is acceptable for commencing business relationship, capital market participant is obliged to introduce "know your client" procedure with the goal to:

- determine if the client has been involved in illegal activities such as frauds, money laundering or organised crime;
- Determine if the prospective client has been penalized for enrolling in terrorist activities, money laundering or other criminal offences.

"Know your client" procedure is fulfilled by delivering of specific form to the client by which client provides information from the paragraph 2 of this article.

Article 4.

Capital market participant is obliged to verify the identity of the client, gather data about customer and transaction (hereinafter: identification) according to the regulation on combating money laundering, especially in following cases:

d) opening owners securities account securities or establishing of some other kind of business relations with the client;
e) of one or more linked transactions amounting to € 15. 000;
f) with every transaction, irrespective of value of such transaction when there are reasonable grounds for suspicion of money laundering in regard to transaction or a client.

Article 5.

Capital market participant is obliged to verify the identity of a client- natural person, by checking the personal identification document issued by authorised public body (identification card, travelling document or other public document enabling undisputable determination of identity of the natural person), in his presence.

Identification of client- natural person, includes:

- name and surname, date and place of birth, permanent place of residence, number of identification documents and place of issue, type and name of the body who issues personal identification document, unique personal identification number of the person opening the account, commences business relationship or executes a transaction, or a person on whose behalf the account is being opened, business relationship is established or transaction is executed;
- name and surname, date and place of birth, permanent place of residence, number of identification documents and place of issue, unique personal identification number of the person of the authorised person who opens the account, commences business relationship or executes a transaction;
- category and purpose of transaction;
- date of opening of the account or establishing business relationship;
- date and time of executing of such transaction;
- amount of transaction;
- way of executing a transaction.

Article 6.

Capital market participant shall establish and verify the identity of a client - legal entity by having insight into the original or certified copy of the document from the Central Register of the Commercial Court (hereinafter: CRCC) or other appropriate public register, submitted by an authorised person on behalf of a legal person, that may not be older than three months of its issue date.
Identification of the client- legal person, includes:

- the firm, residence, unique registry number, tax identification number (hereinafter: PIB) of the legal person opening the account, establishing business relations, or the person on whose behalf the account is being opened, business relation established or transaction executed;
- category and purpose of transaction;
- date of opening of the account or establishing business relationship;
- date and time of executing of such transaction;
- amount of transaction;
- way of executing a transaction.

Capital market participant may establish and verify the identity of the client – legal entity and obtain data from the article 71 item 1 of the Law and by having insight at CRPS or o other appropriate public register . At the statement from the register into which insight has been made the date and time, as well as the name of the person who had an insight is stated.

The data from article 71, items 2, 7, 9, 10, 11, 12, 13, 14 of the Law capital market participant obtains by having insight into the originals or verified copies of documents and other business documents. If by insight in certificate and documents is not able to obtain the data needed, missing data is obtained directly from the agent or authorised person, by insight into documents and business documents which is presented by authorised person. If the missing data, for objective reasons, may not be obtained in the prescribed manner, authorised person is obliged to determine them by written statement of authorised person.
If an reporting entity, when establishing and verifying the identity of a customer, doubts the accuracy of obtained data or veracity of documents and other business files from which the data

have been obtained, he shall request a written statement from the agent or authorised person before establishing business relationship or executing a transaction.
Capital market participants may refuse to establish business relationship with the client or executing of such transaction, if regardless of taking measures from this article, there are still serious doubts about identity of the beneficial customer.

Article 7.

During identification pursuant article 6 of these instruction capital market participants on shall take following procedures:

a) before establishing business relationship or executing transaction determine and verify the identity of a client and identity of beneficial owner on the basis of documents, data and information enabling determination of the identity in doubtless and assertive way;
b) taking measures enabling checking and determining ownership structure of the client and real control over the client in order to determine identity of the beneficial owner client;
c) obtain and keep data and documents in order to establish identity and risk factor of a customer;
d) constantly monitor business relationship with the client, including transaction during that relationship (are they adjusted to the kind of business and risks regarding client and information about that customer) keeping records on monitoring business relationship;
e) If possible, before establishing business relationship with the client, establish reasons for terminating contracts with other participant on the capital market;
f) During executions transactions of customer who is identified with technology help that not include direct contact, enforce procedures that enable previous authenticity checks verity of instruction transaction and authenticity of their applicators.

Article 8.

Person who receives instruction on behalf and for the account of the capital market participant is obliged to identify the customer (employees in the back office).

Article 9.

If client changes a bank, employee is obliged to determine if there was any transaction through the account of the previous bank, if individual or multiple related transactions exceed legally prescribed census.

It is considered that employee has acted in accordance with the paragraph 1 of this article if it obtained statement about stated facts.
When customer during execution of the transactions is changing bank and the amount of transaction below 15.000 € employee is obliged to keep records and deliver all needed data to authorised person.

Article 10.

When customer manages non-money transactions, or transfers of securities without payment, as pursuant contract on gifts, resolutions on inheritance and other resolutions and decisions of the courts, the procedure is as follows:

a) for transfers pursuant enforcement statements of the courts on inheritance in accordance with the law and certified contracts on gifts within first and second inheritance line, employee is not obliged to deliver data to the authorised persons;

b) for transfers pursuant contracts on gifts where person giving and person accepting a gift are not within first or second line of inheritance, employee is obliged to register the client and all needed data deliver to the authorised persons;

Article 11.

During establishing business relationship or executing transaction by agent or authorised person (agent), capital market participants are obliged to identify authorised person,(agent, attorney) and client on whose behalf and for whose account the account has been opened or transaction executed, solely on the basis of personal and another public certificate that are:

- Certificate properly issued by state body within their own competence, or institution or other legal entity within transferred public authority and
- Written authorisation- power of attorney, certified by notary, consulate, court or state administration body.

If, during establishing and verifying the identity of a authorised person, an reporting entity doubts the accuracy of the obtained data and especially in cases when:

- Written authorisation was given to the person who evidentially does not have close relations (family, business etc.) with the customer to perform transaction using customer account;
- When financial state of the customer is known, and funds at the customer account or regarding to this account are not adjusted to his financial state;
- When during business relationship with customer notices some unusual transactions;

he is obliged to obtain his written statement.

Capital market participants can refuse to establish business relationship with the client or to execute specific transaction if, regardless of taking measures prescribed by this article, there are still serious doubts about identity of beneficial customer.

Article 12.

To determine politically exposed persons and members of their close family and close associates by Law, Capital market participants may act on some of the following ways:

e) By filing the written form by the customer;
f) Collecting information from public sources;
g) Collecting information based on insight on data bases that includes the lists of politically exposed persons (*World Check PEP List*, etc).

Procedure of determining close associate of politically exposed persons is followed if the relationship with associate is publicly known or if capital market participant has reason to think that relationship exists. Therefore, during determining the persons who are considered as a close associates of politically exposed persons, capital market participants are not expected to take active researching about this.

Before establishing business relationship with politically exposed person, participant of securities market is obliged to:

- Collect data about founding sources and property which are object of business relationship, transactions, from personal and another identification of customer, and if it is not possible to obtain such a data from the statements submitted, there are collected directly from written statement of the client;
- Obtain written approval of responsible person according to internal acts of the participant before establishing business relationship with customer.

Approval of person responsible pursuant to article 3 item 2 is given in written, in printed or in electronic form.

After establishing business relationship with politically exposed person, members of his close family and close associates by Law, Capital market participants is obliged to keep records about this persons and transactions which are taken on behalf and for the account of those persons.

After obtaining the approval from authorised person there is no need for approval of executing each transaction on behalf and for the account of the client, but capital market participant is obliged to follow transaction with special attention and other business activities by a politically exposed person within organisation and, if needed, notify authorised person in the shortest possible deadline about those transactions.

It is considered that a need determined in the Article 6 exists if transaction is not adjusted to the sources of funds on client's account.

The capital market participant are obliged to ordinarily update their lists of politically exposed persons in order to implement procedures of enhanced customer verification according to Law for the client who, in time of establishing business relationship were not politically exposed persons according to Law.

The capital market participant are obliged to keep the data about politically exposed persons in electronic form.

Article 13.

In order to enable timely and proper delivering of data to Administration for Prevention of Money Laundering and Terrorist Financing in accordance to the law, capital market participant, is obliged to keep records about all persons and transactions and to keep data and documents regarding opening of the account, establishing business relationship and execution of the transaction in written and electronic form at least ten years from the date of execution of such transactions or termination of business relationship.

The authorised person of capital market participant daily makes and in electronic form keeps special records about persons and transactions that are exceeding amount of 15.000 €.

Daily reports about persons and transactions are delivered once a monthly to responsible person of capital market participant t, until 5th of month for preceding month.

Article 14.

The data and information about transactions obtained during implementation of the Law on the prevention of money laundering and documents related to suspicious transactions and accompanying information is considered a secret and is kept apart from the rest of data and documents.

Degree of secrecy, depending on kind of data and documents, is determined by the authorised body of the capital market participant t as:

– „business secret“: limited access for authorised person, members administrative and supervisory bodies and managing bodies and employees at capital market participants or other persons;
– „confidential“: limited access for authorised person and members of administrative and supervisory bodies and managing bodies.
– “top confidential“: limited access for authorised persons and members of administrative bodies.

Access to secret data that are considered as a „business secret“, „confidential“„top confidential“ may be provided, beside authorised person, to the person to whom the license has been issued by authorised body of capital market participant, who may not be a client to whom data are referring or the third person.

Article 15.

Petition for issuing a license to access to secret data is delivered to authorised person of the capital market participant who is obliged to decide about petition in the shortest possible period of time and according to conditions referred to Law.

With decision from paragraph 1 of this article a way of access to this data is determined.

Article 16.

This Instruction shall come in to effect the next day following the date of its delivering to capital market participants.

CHAIRMAN OF THE COMMISSION
Zoran Đikanović, Ph.D

6. THE GUIDELINES ON DEVELOPING RISK ANALYSIS WITH A VIEW TO PREVENTING MONEY LAUNDERING AND TERRORIST FINANCING

September 2009

In relation to the Article 8 paragraph 3 of the Law on the Prevention of Money Laundering and Terrorist Financing (Official Gazette of Montenegro No. 14/07) and Article 2 of the Rulebook on developing risk analysis guidelines with a view of preventing of money laundering and terrorist financing**,** (Official Gazette of Montenegro No.20, from 17th March 2009)

The Administration for the Prevention of Money Laundering and Terrorist Financing established

The Guidelines on developing risk analysis with a view of preventing of money laundering and terrorist financing

LEGAL FRAMEWORK

- Law on the Prevention of Money Laundering and Terrorist Financing (Official Gazette of Montenegro No. 14/07)

- Rulebook on manner of work of the compliance officer, the manner of conducting the internal control, data keeping and protection, manner of record keeping and employees professional training (Official Gazette of Montenegro No. 80 from 26th December 2008)

- Rulebook on the manner of reporting cash transactions exceeding €15,000 and suspicious transactions to the administration for the prevention of money laundering and terrorist financing (Official Gazette of Montenegro 79, from 23rd December 2008).

- Rulebook on developing risk analysis guidelines with a view of preventing of money laundering and terrorist financing (official gazette of Montenegro, no. 20, from 17th March 2009)

This guidelines shall define closer risk factors based on which the level of risk of a client, group of clients, business relationship, transaction or production relation to which the reporting entity shall design internal procedure on risk analysis.

The APMLTF shall, in accordance with the Article 86, paragraph 1, item 8 of the Law on the Prevention of Money Laundering and Terrorist Financing (hereinafter: the Law), conduct supervision on implementation of the Law and its regulations, within its established competences, in accordance with the law on inspection control and in relation to reporting entities from Article 4, paragraph 1, items 15:
16) humanitarian, nongovernmental and other non-profit organisations, and
17) other business organisations, legal persons, entrepreneurs and natural persons engaged in an activity or business of:
- sale and purchase of claims;
- factoring;
- third persons' property management;
- issuing and performing operations with payment and credit cards;
- financial leasing;
- travel organisation;
- real estate trade;
- motor vehicles trade;
- vessels and aircrafts trade;
- safekeeping;
- issuing warranties and other guarantees;
- crediting and credit agencies;
- granting loans and brokerage in loan negotiation affairs;
- brokerage or representation in life insurance affairs, and
- Organising and conducting biddings, trading in works of art, precious metals and precious stones and precious metals and precious stones products, as well as other goods, when the payment is made in cash in the amount of € 15.000 or more, in one or more interconnected transactions.

Basic principles of the fight against money laundering and terrorist financing

1. Establishing and verifying client's identity

Before establishing the business relationship or executing the business transaction, reporting entities are obliged to collect necessary data on a client or to carry out client's identification.
The client's identification is a procedure which includes:
1) establishing client's identity, or if the client's identity has been previously confirmed, to conduct verification of client's identity based on authentic, independent and objective sources;
2) collecting data on a client, of if these data are collected, verification of collected data based on authentic, independent and objective sources.

The reporting entity shall, for a client who is a natural person, or its legal representative, entrepreneur or natural person performing activities, establish and verify client's identity, by insight into the personal identification documents, in client's presence and collect data from Article71, item 4 of the Law. If the required data can not be established from the submitted personal documentation the missing data are collected from other relevant public document submitted by a client.
The client's identity from paragraph 1 of this Article can also be established on the basis of client's qualified electronic certificate issued by a certificate service provider in accordance with the regulation on electronic signature and electronic business.
The reporting entity shall, within procedure of establishing and verifying client's identity, in accordance with the manner prescribed by paragraph 2 of this Article, register data on a client from the qualified electronic certificate into data records from Article 70 of the Law. The data, which can not be collected from client's qualified electronic certificate, shall be collected from the copy of personal documentation which a client submits, in written form, to the reporting entity or in electronic form and if in this manner all required data can not be obtained, the missing data shall be obtained directly from the client.
The electronic service providers, from paragraph 2 of this Article, which issued the qualified electronic certificate, shall upon the reporting entity's request, without delay, provide data on the manner in which they established and verified the identity of the client who possess the qualified electronic certificate.
Establishing and verifying client's identity by usage of qualified electronic certificate is not allowed in the following cases:
1) in the process of opening account at the reporting entities from Article4, paragraph 2 items 1 and 2 of the Law, except when the client is opening temporary depository account for depositing the nominal capital;
2) If there are suspicions that the qualified electronic certificate is misused, or if the reporting entity establishes that the circumstances, which can significantly influence on the certificate's validity, has changed.

If the reporting entity in the process of verifying and establishing client's identity suspect the validity of the collected data or authenticity of documents from which the required data are obtained, than the reporting entity is obliged to require the written statement from the client.
The reporting entity establishes and verifies client's identity from Article 71 item 1 of the Law with insight into original or verified copy of the document from the Central Register of the Commercial Court (hereinafter: CRCC)or other available public registry, which are submitted by an authorised representative and on behalf of the legal person.
The document from paragraph 1 of this Article shall not be older than three months since the issuance date. The reporting entity can establish and verify identity of a legal person and obtain data from Article 71 item 1 of the Law and with insight into CRCC or other available public registry. The reporting entity shall, on the certificate from the registry, which has been viewed, write date and time and personal number of a person which had insight into documentation. The certificate from the business register shall be kept in accordance with the Law.
The reporting entity shall obtain data, from Article 71 items 2, 7, 9, 10, 11, 12, 13 and 14 of this Law, with insight into original documents or verified copies of the documents and other business documentation. If it is not possible to establish data with insight into certificates and documentation, the missing data shall be obtained directly from the representative or authorised person.
If the reporting entity in the process of verifying and establishing client's identity suspects the validity of the collected data or authenticity of certificates and other business documentation from which the required data are obtained, than the reporting entity, before establishing business

relationship or before executing the transaction, is obliged to require the written statement from the representative or authorised person.

If the client is a foreign legal person, performing business activities in Montenegro through its subsidiary, than the reporting entity shall establish and verify the identity of the foreign legal person and its subsidiary.
The reporting entity shall establish and verify the identity of the legal representative and obtain data from Article 71 item 2 of the Law. The data shall be obtained with insight into the personal certificate of the legal representative and in the presence of the legal representative. If it is not possible to establish data with insight into personal certificate of the legal representative, the missing data shall be obtained from other public documents submitted by the legal representative or authorised person.
If the reporting entity in the process of verifying and establishing identity of the legal representative suspects the validity of the collected data, than the reporting entities obliged to require the written statement from the legal representative.

In case when the client's identity can not be established or verified, the reporting entity can not conclude the business relationship or execute the transaction. The reporting entity shall cease all current business relationships with this client.

2. Implementation of the Law and standards

The reporting entities, in the process of performing business activities for which they are registered, are obliged to act in accordance with the adopted laws and by laws that regulate the area of disclosure and prevention of money laundering and terrorist financing. Also, the reporting entities shall ensure that required measures are incorporated into reporting entities performances at all levels.

The legislation in the area of the prevention of money laundering and terrorist financing in Montenegro is harmonised with the relevant regulations in the area of the prevention of money laundering and terrorist financing.
1. Council Directive of 10 June 1991 on prevention of the use of the financial system for the purpose of money laundering (91/308/EEC)
2. Directive 2001/97/EC of the European Parliament and of the Council
Of 4 December 2001 amending Council Directive 91/308/EEC on prevention of the use of the financial system for the purpose of money laundering
3. Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing
4. FATF Recommendations (40+8+1)
5. The United Nations Convention against Corruption (UNCAC)

The Council of Europe through its MONEYVAL Committee also accepts the mentioned documents as referent in its evaluations.

3. Co-operation with the Administration for the Prevention of Money Laundering and Terrorist Financing

In accordance with the Law, reporting entities are obliged to ensure the full co-operation with the supervisory bodies. The obligation related to co-operation between the reporting entities and

supervisory bodies is very significant in cases of providing required data, information and documentation, that refer to the clients or transactions for which there are reasons to suspect in money laundering or terrorist financing. Also, the co-operation is necessary in case of giving information related to behaviour or circumstances that could be connected to, money laundering or terrorist financing and that could harm the safety, stability and reputation of the financial system of Montenegro.
Due to that the realisation of the internal procedures can not, in any case, directly or indirectly, limit the co-operation between the reporting entities and the APMLTF or in any other manner influence on the co-operation efficiency.

4. Adoption of internal procedure

The reporting entities shall adopt the unique policy of risk management in combating money laundering and terrorist financing, and due to that adopt the internal procedures, particularly in the area of: client's verification, risk analysis, recognising clients and transactions for which there are reasons to suspect in money laundering and terrorist financing. It is particularly important that all employees are informed about the procedures, to act in accordance with the procedures and to use them in their daily work.

The content of internal procedures developed by the reporting entities:
A) manner of establishing client's acceptability;
b) risk assessment of groups and clients;
c) the manner of establishing the risk of product and services, with the view of the prevention of money laundering and terrorist financing;
d) manner of client's identification;
e) client's accounts and transactions supervision;
f) managing risks to which the reporting entities are exposed, in the area of the prevention of money laundering and terrorist financing;
h) training programs for employees.

5. Professional training

The reporting entity is obliged to provide, on regular basis, professional training and qualification of all employees that directly or indirectly perform activities of prevention or concealing money laundering and terrorist financing.

RISK ASSESSMENT

1. The purpose of risk assessment

In accordance with the Law, the risk on money laundering and terrorist financing is the risk that the client is going to misuse the financial system of Montenegro for money laundering and terrorist financing or that a certain business relationship, transaction or product is going to be directly or indirectly used for money laundering and terrorist financing.
The reporting entity shall, in accordance with the Law and in order to prevent exposure to money laundering and terrorist financing, make risk assessment through which the level of client, business relationship, product or transaction's exposure to risk will be determined
The risk analysis preparation is a necessary precondition for performing the prescribed client's verification measures. The classification of the client, business relationship or transaction in one risk category depends on the type of client's verification which the reporting entity is obliged to

perform in accordance with the Law (enhanced customer due diligence, simplified customer due diligence and simplified customer due diligence)

2. Risk management policy and risk analysis

The reporting entity or its management can, for the necessity of more efficient implementation the provisions of the Law and Guideline, before the risk analysis preparation, adopt adequate risk management policy for the prevention of money laundering and terrorist financing. The purpose for adopting this policy is primary to determine, 0n the level of reporting entities, the areas of business activities that are, due to possibility of misuse for money laundering or terrorist financing, more or less critical, or for the reporting entities to establish and determine the main risks in this areas and measures for their solution. The reporting entities shall, during the process of developing the starting basis for adoption the policy for money laundering or terrorist financing risk management, take into consideration the following criteria that, in the process of designing the policy, defines details on:
1. the purpose and aim of money laundering and terrorist financing risk management and its connection with the reporting entities' business aims and strategy,
2. the reporting entities' areas and business processes that are exposed to money laundering and terrorist financing risks,
3. money laundering and terrorist financing risks in all key business areas of the reporting entities,
4. measures for resolving money laundering and terrorist financing risks,
5. the role and responsibility of the reporting entities management in the process of performing and adoption of money laundering and terrorist financing risk management.

3. Risk analysis preparation

Risk analysis is a procedure in which the reporting entity defines:
- evaluation of probability that the reporting entities' business activities can be misused for money laundering and terrorist financing
- criteria, based on which the certain client, business relationship, product or transaction will be classified in to category of clients that are more or less exposed to money laundering and terrorist financing clients,
- establishing consequences and measures for efficient managing of these risks.

The reporting entity shall, in the process of risk analysis preparation, take onto consideration the following criteria:
1. the reporting entity is obliged to develop the risk criteria so that the specific client, business relationship, product or transaction is determined in one risk category.
2. the reporting entity can, in the process of determine risk category, in accordance with its risk management policy, classify, on their own, the certain client, business relationship, product or transaction category as the category exposed to high risk of the money laundering and terrorist financing and perform enhanced due diligence,
3. the reporting entity may not, in the process of determining the certain client, business relationship, product or transaction risk category, that are in accordance with the Law and Guidelines determined as high risk clients, classify as middle(average)or low risk clients.

4. Preparation of risk evaluation

4.1. Initial risk establishment

The reporting entity shall, based on risk analysis, prepare the risk evaluation of each customer-client, business relationship, product or transaction; before closing business relationship or executing business transaction it is necessary:

1. To establish client's identification through obtained data that are required on client, business relationship, product or transaction and other data which the reporting entity is obliged to obtain.
2. to evaluate obtained data with the view of risk criteria for money laundering or terrorist financing (risk establishment)
3. to determine the evaluation of the risk of the client, business relationship, product or transaction, which must be based on previously established risk analysis, through the classification of the costumer, business relationship, product or transaction into one of the risk categories
4. performs measures of enhanced customer risk analysis (enhanced CDD, simplified CDD and usual CDD)

4.2. Subsequent risk assessment

The reporting entity shall, within measures of regular supervision of the business relationship with the costumer, verify, again, basis for the initial evaluation of the costumer or business relationship, by which the reporting entity evaluated the costumer and if it is necessary, the reporting entity shall define the new risk assessment (or subsequent risk assessment). The reporting entity shall subsequently assess the initial risk evaluation of a certain customer or business relationship in the following cases:
1. if the circumstances, on which the evaluation of a certain customer or business relationship is based, has changed significantly; or if the circumstances, that significantly influence on the classification of costumer or business relationship into risk category, change,
2. If the reporting entity suspects the validity of data, based on which a certain costumer or business relationship has been classified into the specific risk category.

5. Criteria for defining customer risk category

The reporting entity shall, in the process of defining risk evaluation of a customer, business relationship, product or transaction, take into account the following criteria:
1. type, business profile and structure of client
2. geographical origin of the customer
3. the nature of business relationship, product or transaction
4. Previous experiences of the reporting entity in relation to a client.

In the process of defining customer risk category, the reporting entity can, besides the mentioned criteria, observe other criteria for defining the level of risk for a certain costumer, product or transaction:
1. size, structure and business activity of the costumer, including the scope, structure and complexity of business activities which costumer carries out on the market,
2. status and ownership structure of costumer

3. costumer's presence during the process of closing business activity or executing transaction,
4. source of assets that are subject of the business relationship or transaction in case if the costumer is, in accordance with criteria prescribed by the Law, defined as politically exposed person
5. purpose of closing business relationship or execution of business transaction,
6. costumer's knowledge on product and its experience or knowledge on this area,
7. other information showing that costumer, product or transaction could have high risk.

6. Costumer risk categories

In relation to risk categories costumer, business relationship, products and transactions can be classified into 4 main risk categories, as follows:

1. extremely high risk, due to which the business with costumer is prohibited,
2. high risk,
3. Medium (average) risk
4. Low risk.

6.1. Prohibition on conducting business activities with a customer

Conducting business activities with the following costumers is prohibited due to direct and high risk on money laundering or terrorist financing:
1. customers (legal and natural persons and other subjects) that are listed as persons against whom UN Security Council or European Union measures are taken- these relevant measures are: financial sanctions that include freezing assets on the account and /or prohibition on assets usage (economical sources), military embargo which means prohibition on arms trafficking with the mentioned subject etc.
2. customers with the residence or head office inanities that are not subject to the international law or not internationally recognised sovereign states (these entities give the possibility of fictive registration for legal persons, allow issuing fictive identification documents etc.)

Prohibition on executing transactions and closing business relationship with a customer is applied in the following cases:
1. transactions were intended to be sent to persons or subjects against which UN Security Council or European Union imposed measures
2. transactions that customer would execute on behalf of person or subject against which UN Security Council or European Union imposed measures
3. business relationships that would be concluded on behalf of a person or subjects that are listed as persons against whom UN Security Council or European Union imposed measures

6.2. High risk of money laundering or terrorist financing

6.2.1. Type, business profile and structure of customer

The high risk of money laundering and terrorist financing costumers is as follows:

Natural persons:

Customer is politically exposed person or person that is acting or has been acting in the last year on a prominent public position in a state, including his/her immediate family members and close associates, as follows:
1. presidents of states, prime ministers, ministers and their deputies or assistants, heads of administration authority and authorities of local governance, as well as their deputies or assistants and other officials;
2. elected representatives of legislative authorities;
3. holders of the highest juridical and constitutionally judicial office;
4. members of State Auditors Institution or supreme audit institutions and central banks councils;
5. consuls, ambassadors and high officers of armed forces, and
6. members of managing and supervisory bodies of enterprises with majority state ownership

Marital or extra-marital partner and children born in a marital or extra-marital relationship and their marital or extra-marital partners, parents, brothers and sisters shall be deemed immediate family members of the politically exposed person.

A natural person that has a common profit from the asset or established business relationship or other type of close business contacts shall be deemed a close assistant of the politically exposed person.

Legal persons:

a. customer is a foreign legal person that does not conduct or is not allowed to conduct trade, production pr other business activities in the country in which it is registered (legal person with head office in the state that is known as off shore financial center and for which there are a certain limitations when performing direct business registration in that country)
b. customer is fiduciary (trust) or other similar company of the foreign legal person with unknown or disguised owners or management team (company of foreign legal person that provides conducting business activities for third persons i.e. companies established on the basis of legal agreement between founder and manager that governs the founder's property, on behalf of certain persons that are users or beneficiaries or for other purposes(from private gained assets to general assets that are not gained),
c. customer has a complicated status structure or complex ownership chain (complicated ownership structure or complex ownership chain disables or does not allow establishment of the beneficiary owner of legal person),
d. customer is organisation that, for conducting its business activities does not need or is not obliged to get license from the competent supervising body; or in accordance with the national legislation customer is not subject to measures of detection and prevention of money laundering and terrorist financing,
e. customer is non profitable organisation (institution, company or other legal person or entity established for publicly useful, charity purposes, religious communities, association, foundation, non profit association and other persons that do not perform economic activity) and fulfils one of the following conditions:

1. has a registered office in the state known as off shore financial center
2. has a registered office in the state know as financial or tax paradise
3. has a registered office in the non EU member state or did not sign EU pre accession agreement

4. among its members or founders is a natural or legal person which is resident of any of the states mentioned in the previous item.

6.2.2. Geographical position of customer

The customers that present high risk from money laundering and terrorist financing are included in customers with the permanent residence or registered office:

1. in the state that is non EU member state or did not sign EU pre accession agreement,
2. in the state that is, based on assessment of the competent international organisations, known for production or well organised drug trafficking (Middle and Far East countries known for heroin production: Turkey, Afghanistan, Pakistan and golden triangle countries (Myanmar, Laos, Thailand), South American Countries known for cocaine production Peru, Columbia and neighbor countries, Middle and Far East Countries, Central American Countries known for Indian hemp production: Turkey, Lebanon, Afghanistan, Pakistan, Morocco, Tunis, Nigeria and neighbor countries, Mexico),
3. state that is, based on assessment of the competent international organisations, known as country with high level of organised crime due to corruption, arm trafficking, human trafficking or human rights violation,
4. state that is, based on assessment of the international organisation FATF (Financial Action Task Force) classified in to the non cooperative countries or territories (that are countries and territories that, according to FATF assessment, do not have relevant legislation in the area of prevention and detection of money laundering or terrorist financing, the state supervision of financial institutions does not exist or it is not relevant, establishing and acting of the financial institutions is possible without state certificates or registration at the competent authorities, state supports opening anonymous accounts or other anonymous financial instruments, the system of recognising and reporting suspicious transactions is inappropriate, the establishing beneficial owner is not an obligation prescribed by the law, international co-operation is not efficient or does not exists at all)
5. country against which UN or EU measures are imposed, including complete or partial break up of economic relations, railways, waterways, post, telephone lines, telegraph lines, radio and other communicational relations, breakup of diplomatic relations, military embargo, travel embargo etc.
6. country which is known as financial or tax paradise (for these countries it is particularly important that they enable complete or partial tax free obligation, or tax rate is significantly lower than tax rate in other countries. These countries usually do not have concluded agreements for the avoidance of double taxation, or if they do sign the agreements, they do not obey them. The legislation of these countries requires strict observance of bank and business secrecy and also quick, discreet and cheap financial services are provided. Countries known as financial or tax paradises are : Dubai – Jebel Ali Free Zone, Gibraltar, Hong Kong, Isle of Man, Lichtenstein, Macau, Mauritius, Monaco, Nauru, Nevis Island, Iceland –Norfolk Area, Panama, Samoa, San Marino, Isle of Sark, Seychelles, St. Kitts and Nevis, St. Vincent and Grenadine, Switzerland – canton Vaud and Zug, Turks and Caicos Islands, the USA – federal states Delaware and Wyoming, Uruguay, British Virgin Islands and Vanuatu
7. country known as offshore financial center (these countries define certain limitations in the process of direct activities registration of business entities in the country, provide high level of bank and business secrecy, liberal control over international trade business is performed, quick, discreet and cheap financial services and legal person registration are enabled. It is significant that these countries do no not have adopted relevant legislation in the area of prevention and detection of money laundering and terrorist financing. Countries known as offshore financial centers are: Andorra, Angola, Antigua and Barbuda, Aruba, Bahamas, Barbados, Belize, Bermudas, British Virgin Islands, Brunei Darussalam, Cape Verde, Cayman Islands, Cook Islands, Costa Rica,

Delaware (USA), Dominica, Gibraltar, Grenada, Guernsey, Isle of Man, Jersey, Labuan (Malaysia), Lebanon, Lichtenstein, Macao, Madeira (Portugal), Marshall Islands, Mauritius, Monaco, Montserrat, Nauru, Nevada (USA), The Netherlands Antilles, Niue, Palau, Panama, Philippines, Samoa, Seychelles, St. Kitts and Nevis, St Lucia, St Vincent and Grenadines, Zug (Switzerland), Tonga, Turks and Caicos Islands, Uruguay, Vanuatu and Wyoming (USA).

Reporting entities should consider the following International organisations as competent for supervising the efficient measures implementation in the area of prevention of money laundering and terrorist financing and its harmonisation with international standards:

1. European Bank for Reconstruction and Development
2. Committee on the Prevention of Money. Laundering and Terrorist Financing of the European Commission,
3. Financial Action Task Force on Money Laundering (FATF),
4. International Monetary Fund
5. World Bank
6. The Egmont Group is an international network of national Financial Intelligence Units specialized in the combating of money laundering and terrorist financing
7. Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism – MONEYVAL
8. International Organisation of Securities Commissions (IOSCO)
9. The Committee of European Securities Regulators (CESR),
10. Committee of European Insurance and Occupational Pensions Supervisors(CEIOPS),
11. International Association of Insurance Supervisors (IAIS).

6.2.3. Business relations, products and transactions

Business relations that could represent high risk of money laundering and terrorist financing include:

1. business relations that include permanent and high amount assets payment from the costumer's accounts, or towards credit or financial institution in non- EU member states, or country which did not sign EU Pre-Accession Agreement, or business relations that include higher payments to the customer's account opened at credit or financial institution in non- EU member states, or country which did not sign EU Pre-Accession Agreement,
2. business relations that a foreign credit financial institution or other fiduciary institution performs, on behalf of the customer and as its representative, with registration office in non- EU member states, or country which did not sign EU Pre-Accession Agreement,
3. business relationships concluded without the simultaneous physical presence of customer, and due to that the conditions for simplified CDD are not fulfilled,

Transactions that could represent high risk of money laundering and terrorist financing include:

1. payment from customer's account or payment to customer's account, which differ from the account that customer provided in the process of identification of the account through which customer regularly carried or has been carrying business activities (particularly in case of crossbred transactions)
2. transactions intended to be sent to a persons with the residence or registered office in country known as financial or tax paradise,
3. transactions intended to be sent to a persons with the residence or registered office in country known as off shore financial center,
4. transactions intended to be sent to non profit organisations with the registered office in: country known as off shore financial center, country known as financial or tax paradise or in non-EU member states, or country which did not sign EU Pre-Accession Agreement,

6.2.4. Previous experiences of the reporting entity with a customer

Customers that, regardless to the reporting entity's experience, present a high risk of money laundering and terrorist financing are as follows:
1. persons in relation to whom, within past three years, the Administration for the Prevention of Money Laundering submitted request on temporary suspension of a suspicious transaction to the reporting entity,
2. persons in relation to whom, the Administration for the prevention of Money Laundering and terrorist Financing submitted request for ongoing monitoring of customer's financial activities to the reporting entity
3. Persons for which, within past three years, the reporting entity submitted data to the Administration for the Prevention of Money Laundering and terrorist financing, since, in relation to that person or transaction that this person executed, there are reasons for suspicion in money laundering and terrorist financing.

*6.3. Medium (**average**) risk of money laundering and terrorist financing*

Reporting entity classifies in the category of middle (average) risk the customers whose business relationship, product or transaction, based on the Guidelines criteria, can not be classified as high or low risk customers

6.4. Low risk of money laundering and terrorist financing

Reporting entity shall classify the following customers as customers with low risk of money laundering or terrorist financing:
1. customers from Article 4, paragraph 2 of the Law

- companies for managing investment funds and branches of foreign companies for managing investment funds of other countries, companies for managing investment funds of member states that opened its branches in Montenegro or which are authorised for direct managing investment funds in Montenegro or third persons that are, in accordance with the Law that defines funds business activities, authorised by company for managing investment fund to perform certain business activities,
- companies for managing pension funds and branches of foreign companies for managing pension funds and insurance companies;
- companies authorised to deal in financial instruments and branches of foreign companies for dealing in financial instruments in Montenegro,
- insurance companies, authorised for dealing with life insurance, branches of foreign insurance companies, from third countries, authorised for dealing with life assurance and insurance companies from the member states, that directly or through branches deal with life insurance in Montenegro, or other same institution fulfilling condition to possess registered office in the member state or third country

2. state body, local government body or other legal persons performing public competences
3. company whose financial instruments are accepted and traded at stock market or organised public market in one or more member states and in accordance with EU regulations or companies with registered office in the third country whose financial instruments are accepted and traded at stock market or organised public market in the member state or in the third country,

under the condition that in the third country the requests for data publication, in accordance wit EU regulations, are in force.

CUSTOMER DUE DILIGENCE

1. Regular customer due diligence

Customer due diligence is the key preventive element in the system of detecting money laundering and terrorist financing. The purpose of customer due diligence measures is to credibly establish and confirm the true identity of the customer. Customer due diligence includes: establishing and analysing the identity of a customer, establishing the beneficial owner of a customer when the customer is a legal person and the data on the purpose and intended nature of a business relationship or transaction and other data, in accordance with the provisions of the articles 7, 15, 16, 17, 20 of the Law.

A reporting entity shall establish and verify customer's identity on the basis of reliable, independent and objective sources (by checking the appropriate ID document).

It is forbidden to establish a business relationship or carry out a transaction in cases when it is not possible to identify the customer, or when the reporting entity has reasonable grounds to suspect the authenticity or credibility of the data, or the documents used by the customer for proving his/her identity, or when the customer is not ready or does not show readiness to cooperate with the reporting entity in establishing the authentic and complete data required by the reporting entity when it applies customer due diligence procedure. In such cases the reporting entity may not establish a business relationship, or it shall terminate the existing relationship or transaction and notify the Administration for the Prevention of Money Laundering and Terrorist Financing on the termination.

The reporting entity may shorten the customer due diligence procedure solely in those cases when there are reasonable grounds to suspect that a customer or transaction are related to money laundering or terrorist financing.

The Law proceeds from the basic assumption that certain customers, business relationships, products or transactions pose higher and others pose lower risks of money laundering or terrorist financing. Therefore for certain cases the Law prescribes especially strict customer due diligence procedures, while for certain cases it prescribes simplified customer verification measures.

2. Customer due diligence obligation

The reporting entity shall carry out customer due diligence in the following cases:

1. when establishing a business relationship with a customer (a business relationship is any business or contractual relationship established or concluded by a customer at a reporting entity and it is related to carrying out the professional activities of the reporting entity, for example, investment contract, stock broker contract, financial instruments management contract, customer's access to the rules of investment fund management, etc.),
2. when carrying out any transaction in the amount of € 15,000 and more, whether the transaction is carried out in a single operation or in several operations which appear to be linked. Under the 'transactions that are logically interlinked' we consider the following:
- two or more successive, separated transactions, amounting to more than € 15,000, executed by a certain customer on behalf of the same third person with the same purpose,

- two or more transactions amounting to more than € 15,000, executed by several persons with family or business links, on behalf of the same third person with the same purpose,

3. when there is suspicion about the accuracy or veracity of the previously obtained data on the customer or the beneficial owner of the customer,

4. in all cases when there are reasons to suspect that a transaction or a customer are related to money laundering or terrorist financing, regardless of the amount of the transaction.

2. Enhanced customer due diligence

When a certain customer, business relationship, product or transaction are considered as highly risky for money laundering or terrorist financing, reporting entities shall apply enhanced customer due diligence measures. As highly risky for money laundering or terrorist financing the Law defines the following: establishing a correspondent relationship with a bank or other similar credit institution that has a registered office in a third country, business relationships established with a politically exposed person and cases where the customer is not present when the establishing and verifying customer identity are made within the application of customer due diligence measures.

2.1. Enhanced customer due diligence for politically exposed persons

According to the provisions of the Law politically exposed persons pose high risk customers. Therefore a reporting entity shall apply enhanced due diligence measures in all cases when a customer is a person defined by the criteria of the Law and the Guidelines as a politically exposed person, before establishing a business relationship or executing a transaction.
Enhanced customer due diligence includes the application of additional measures, such as:
1. collecting data on the source of the funds and property that are or will be the subject of the business relationship, or transaction,
2. mandatory obtaining of a written consent of a superior responsible person before establishing a business relationship with such customer,
3. very careful monitoring of transactions and other business activities carried out by a politically exposed person at the reporting entity, after establishing the business relationship.

A reporting entity obtains information on whether a specific person is a politically exposed person or not on the basis of a signed written statement fulfilled by a customer before establishing a business relationship or executing a transaction (Questionnaire for identifying politically exposed persons). The written statement has to be made in the mother language and in English.

The written statement has to include the following data:

QUESTIONNAIRE FOR IDENTIFYING A POLITICALLY EXPOSED PERSON

In accordance with the Law on the Prevention of Money Laundering and Terrorist Financing (hereinafter: the LPMLTF, Official Gazette of Montenegro, No. 14/07), ____________ (reporting entity) must establish whether a customer is a politically exposed person when entering into a business relationship or executing transactions (Article 9 Paragraph 1 Item 2) with the customer .
A ***politically exposed person*** *is any natural person who works or has worked in the last year in a high-profile public position, including that person's immediate family members and co-workers.*
Immediate family members of a politically exposed person *are spouses or cohabiting partners, parents, brothers and sisters, as well as children and their spouses or cohabiting partners.*

Immediate co-workers of a politically exposed person *are all persons who have joint income from property, an active business relationship or any other form of close business contact.*

Pursuant to the requirements of the LPMLTF, we are kindly requesting that you answer the following questions.

1. Are you:

1.	a head of state?	YES	NO
2.	the head of a government?	YES	NO
3.	a minister or deputy or assistant thereof?	YES	NO
4.	Head of state administrative body or local administrative body, or his /her deputy or assistant and other official?	YES	NO
5.	an elected representative of a legislative body (MPs and other person appointed or elected by the Parliament)	YES	NO
6.	a holder of the highest judicial and constitutional court functions (judges, prosecutors, and their deputies)	YES	NO
7.	a member of a court of auditors or supreme auditing institutions and central bank governing board?	YES	NO
8.	an ambassador?	YES	NO
9.	A consul? (diplomatic agents)?	YES	NO
10.	a high-ranking officer in the armed forces?	YES	NO
11.	a member of the management or supervisory board of a company under majority state ownership?	YES	NO

2. Are you:

1.	An immediate family member of the persons defined in point 1? • Spouse of cohabiting partner • Parent • Brother or sister • Child born in a marital or extramarital relationship and his or her spouse or cohabiting partner	YES YES YES YES	NO NO NO NO
2.	An immediate co-worker of the persons defined in point 1 • Do you have joint income from property or an active business relationship with the persons defined above? • Do you have any other form of close business contact with the persons defined above?	YES YES	NO NO

3. Have you:

In the last 12 months worked in any of the positions set out in point 1?	YES	NO
Are you an immediate family member or co-worker of a person who has worked in any of the positions, set out in point 1, in the last 12 months?	YES	NO

If you have answered YES to any of the above questions, you are considered a politically exposed foreign person according to the law. We therefore kindly request that you state the origin of funds and property that are or will be the subject of the business relationship or transaction:

I, the undersigned, hereby confirm that the above stated data are correct and true.

____

Name and surname of person completing the questionnaire

Customer's address Customer's data of birth

Place and date Signature of the customer

Name and surname of the bank employee

Place and date Signature of the bank employee

I hereby authorise the entering into a business relationship with a politically exposed person.

Name and surname of the responsible senior staff member

Place and date Signature of the responsible senior staff member

In case of suspecting the accuracy of the data obtained in the statement the reporting entity can additionally verify the information by checking the public and other data available to the reporting entity (the reporting entity judges to which extent it will consider the commercial lists, i.e politically exposed persons data bases, credible and relevant for enhanced customer due diligence). Also, the data can be checked at: competent state authority, consular agencies or embassies of foreign countries in Montenegro.

A reporting entity shall pay special attention to any risk of money laundering and/or terrorist financing that could result from technical developments (ex. Internet banking) and put in place policies and undertake measures for preventing the use of new technology developments for the purposes of money laundering or terrorist financing. The reporting entities' policies and procedures for the risk related to a business relationship or transaction with customers that are not physically present, are also applied when doing business with customers through new technologies.

3. Simplified customer due diligence

A reporting entity shall apply simplified customer due diligence in the following cases: when there is insignificant risk of money laundering or terrorist financing, when the data on a customer which is a legal person or its beneficial owner are transparent, or publicly available. This means

that a reporting entity in a certain case establishes and verifies the identity of a customer, but the procedure is simpler than the enhanced customer due diligence procedure.

A reporting entity will not establish a business relationship or execute a transaction before he/she establishes all the facts needed for customer risk assessment.

Simplified customer due diligence is not allowed when there is suspicion that a customer or transaction are related to money laundering or terrorist financing, or when the customer is, according to the risk assessment, categorized as a high risk customer.

4. Customer due diligence conducted by third parties

When establishing a business relationship, a reporting entity can, as a term prescribed by the Law, entrust a third person with customer due diligence procedure, previously verifying has the third person conducting customer due diligence procedure met all the requirements prescribed by the Law and bylaws.

A reporting entity verifies the fulfillment of the requirements by the third person in one of the following ways:

1. checking public or other available data bases,
2. checking the documents and business documentation provided to the reporting entity by the third person, or
3. obtaining a written statement from the third person by which the third person guarantees to the reporting entity that he/she has met the requirements.

If the third person, instead of the reporting entity, has conducted enhanced customer due diligence the third person is responsible for meeting the requirements from the Law, including reporting transactions obligation and the obligation of keeping data and documentation.

Even though the third person has carried out enhanced customer due diligence, instead of the reporting entity, the reporting entity is still responsible for the implementation of enhanced customer due diligence.

IMPLEMENTING THE MEASURES OF DETECTING AND PREVENTING MONEY LAUNDERING AND TERRORIST FINANCING IN BUSINESS UNITS AND COMPANIES IN WHICH A CUSTOMER IS A MAJORITY SHAREHOLDER OR HAS A MAJORITY VOTING RIGHT, AND WHICH HAVE A REGISTERED OFFICE IN A THIRD COUNTRY

A reporting entity establishes a system of conducting unique policy of detecting and preventing money laundering and terrorist financing. For such purposes a reporting entity especially pays attention to implement the detecting and preventing money laundering and terrorist financing measures prescribed by the Law in relation to customer due diligence, suspicious transactions reporting, record keeping, internal audit, nominating an agent, keeping data and other important circumstances related to detecting and preventing money laundering or terrorist financing to the same, or similar extent in the business units and companies where the reporting entity is a majority shareholder or has a majority voting right, and which have a registered office in a third country.

If the implementation of detecting and preventing money laundering and terrorist financing in business units and companies where the reporting entity is a majority shareholder, or has a majority voting right is entirely contrary to the legislation of the third country where the business unit or company have a registered office, the reporting entity shall notify the Administration for the Prevention of Money Laundering and Terrorist Financing and take the appropriate measures for eliminating the risk of money laundering or terrorist financing, such as:

1. putting in place additional internal procedures for preventing, or diminishing the possibility of abuse for the purpose of money laundering or terrorist financing,
2. carrying out additional internal control over the reporting entity's business operations in all the key areas that are most vulnerable to money laundering and terrorist financing,
3. establishing internal risk assessment mechanisms for certain customers, business relationships, products and transactions,
4. implementing strict policy of classifying customers according to the degree of risk related to them and consistent implementation of the measures accepted on the basis of that policy,
5. additional training of the employees.

The Administration shall:

- ensure that all business units and companies where the reporting entity is a majority shareholder or has a majority voting right, and which have a registered office in a third country and their employees get introduced to the policy of detecting and preventing money laundering and terrorist financing,

- ensure, through the director of the business units and companies where the reporting entity is a majority shareholder or has a majority voting right, the internal procedures of detecting and preventing money laundering and terrorist financing, to be substantially integrated into their business processes,

- conducting ongoing monitoring of the appropriate and effective implementation of detecting and preventing money laundering and terrorist financing measures in the business units and companies where the reporting entity is a majority shareholder or has a majority voting right, and which have a registered office in a third country.

MONITORING OF CUSTOMER BUSINESS ACTIVITIES

I. The purpose of customer business activities monitoring

Regular monitoring of the customer business activities is the key for efficiency determination of proscribed measures implementation in the area of money laundering and terrorism financing detection and prevention. The purpose of customer business activities monitoring is to determine the legitimacy of the customer business and to verify the compliance of the customer business activities with provided nature and purpose of business relation which the customer concluded with compliance officer, or with customer's regular scope of work. Monitoring of customer business activities is divided into four different segments of customer's business with compliance officer as follows:

1. Monitoring and verification of customer's business compliance with provided nature and purpose of business relationship;

2. Monitoring and verification of the customer's resources origin compliance with the supposed resources origin which the customer stated when setting up business relationship with compliance officer;
3. Monitoring and verifying compliance of customer's business activities with the customer's usual scope of work;
4. Monitoring and updating of collected documents and data about the customer.

II. Measures of client's business activities monitoring

1. In order to monitor and verify the compliance of customer's business activities with the supposed nature and purpose of business relation which the customer concluded with reporting entity, the following measures are used:

a) Data analysis on purchase and/or selling of financial instruments or other transactions for specific time period with the intention to determine whether, in relation to specific financial instruments purchase or selling or any other transaction, there exist possible circumstances for suspicion on money laundering and/or terrorism financing. Decision on suspicion is based on suspicion criteria determined by the list of indicators for recognising customers and transactions with which there exist reasons for suspicion on money laundering, and/or list of indicators for recognising clients and transactions with the view on reasons for suspicion on terrorism financing,
b) Drafting new customer risk assessment and/or updating previous customer risk level.

2. The following measures are used for monitoring and verification of customer business activities compliance with customer's usual scope of business activities:

a) Monitoring of financial instruments purchase and selling value, and/or other transactions above the specific limit – it is the decision of the reporting entity what would be the specific limit for specific customer above which the business activity of the customer would be monitored. The same is applied for every customer individually bearing in mind in particular the risk based category of customer (for efficient application of this measure the reporting entity may establish adequate information support),
b) Analysis of specific purchase or selling of financial instrument, and/or other transaction with the view of suspicion on money laundering and terrorism financing when the number of selling or purchase of financial instruments exceeds certain amount. Analysis of suspicion of financial instruments purchase or selling and/or other transactions is based on suspicion criteria determined in the list of indicators for recognising suspicious customers and transactions and/or list of indicators for recognising customers and transactions with the grounds for suspicion on terrorism financing.

3. For monitoring and updating of collected documents and data about the customer:

a. yearly customer analysis (simplified and deep and usual),
b. yearly customer analysis (simplified and deep and usual), when there exist a doubt on authenticity of previously received data about the customer or about the real owner of the customer (if the customer is an legal entity),
c. verification of customer data or of customer's legal representative in the court registry or any other public registry,
d. verification of received data within the premise of the customer or it's legal representative or assignee,

e. verification of list of persons, countries and other entities subject to application of UN Security Council measures or EU.

III. The scope of customer's business activities monitoring

The scope and intensity of customer's business activities monitoring depends on risk based approach level of specific customer, and/or categorization of the customer into specific risk category. Adequate scope of monitoring dedicated to business activities of specific customer understands following:

1. In the case when dealing with highly risk customer – determined monitoring measures of customer's business activities leveled as highly risk the reporting entity applies at least once a year. When dealing with highly risk customer the reporting entity regularly, at least once a year, conducts measures of repeated yearly customer analysis (simplified and deep and usual), if certain requirements, determined by the Law, have been met.
2. In the case of medium (average) risk customer – the reporting entity applies determined measures of monitoring customer's business activities at least once in three years. In the case of medium (average) risk customer the reporting entity, regularly, at least once a year, applies measures of repeated yearly customer analysis (simplified and deep and usual), if certain requirements, determined by the Law, have been met.
3. In the case of law risk customer the reporting entity regularly, at least once a year, applies measures of repeated yearly customer analysis, if certain requirements, determined by the Law, have been met.

Customer's business activities' monitoring is not required, if the customer did not carry out business activity (purchase and selling of financial instrument or other type of transaction) after concluding business relation. In this specific case the reporting entity would apply measures of monitoring business activities of the customer, after conducting the first following purchase or selling of financial instrument, and/or performing the following transaction.
In accordance with the policy of money laundering and terrorism financing risk based approach the reporting entity, in internal document, is in position to decide for more frequent monitoring of business activities of specific customer, than determined in the Guidelines and is also in position to establish additional measures to assist monitoring of customer's business activities and to determine the legitimacy of customer's business activities.

DATA DELIVERY

1.Notification on cash transactions

In case when specific customer carries out a cash transaction with the reporting entity, amounting to €15 000 and above, the reporting entity is liable to, in accordance with the Law, immediately after the transaction has been carried out, and/or in time frame of three working days after the transaction has been carried out, deliver data on this specific transaction to Administration for the Prevention of Money Laundering and Terrorism Financing, by fulfilling the form provided in the Rule Book on the Manner of Reporting Cash Transactions Exceeding the Value of €15 000 and Above and Suspicious Transactions to the APMLFT (Official Gazette MN no.79. dated: 23, December 2008.).
Cash transaction is every transaction involving reporting entity accepting cash from the customer (coins and bank notes), and/or delivers cash to the customer amounting to €15 000 and above, regardless the value, that the reporting entity receives from the customer and/or delivers to the customer.

2. Notification on suspicious transactions

2.1. What is suspicious transaction?

The provisions of the Law determine that every transaction may be treated as suspicious if being by its nature, scope, complexity, value and links unusual, and/or without clearly visible economic or legal ground, and/or are not in accordance or in disproportion with usual and/or foreseen business of the customer and other circumstances in relation to status and/or other characteristics of the customer. Specific transactions of the customer and specific business relations as well may be treated as suspicious. The suspicious grade of certain customer, transaction or business relation is based on suspicion criteria determined in the List of Indicators for Recognising Suspicious Clients and Transactions when there grounds for suspicion on money laundering, and/or in the List of Indicators for Recognising Suspicious Clients and Transactions when there grounds for suspicion on terrorism financing. Indicators are basic guidelines to employees/compliance officers when recognising suspicious circumstances in relation to specific customer, transaction carried out by the customer and/or business relation having concluded, therefore all employees with the reporting entity need to be familiar with Indicators in order to be able to use them in their work. When deciding whether the transaction is suspicious the compliance officer needs to provide any professional assistance to other employees.

Employees with reporting entity determining that there are reasonable grounds for suspicion on money laundering and/or terrorism financing need to notify the compliance officer for money laundering prevention or his/her deputy about this founding. The reporting entity needs to organise the procedure of suspicious transaction reporting between all organisational units and compliance officer, in accordance with the following instructions:

1. precisely determine the manner of data delivering (telephone, fax, secure electronic manner etc.),
2. determine the type of data being delivered (data about customer, reason for suspicion on money laundering etc.),
3. determine the manner of co-operation between organisational units with compliance officers,
4. determine the manner of treating customer when the APMLFT is temporarily blocking transactions,
5. determine precise role of compliance officer when reporting suspicious transaction,
6. prohibit data discovery about the situation that data, information or documents is or would be reported to the APMLFT,
7. determine measures related to continuation of business relation with customer (temporary ceasing of business relation, ceasing of business relation, performing measures of deep customer analysis and detailed monitoring of future business activities of the customer etc.).

Notification on suspicious transaction needs to be delivered to APMLFT before carrying out of business transaction was performed (telephone, fax or some other appropriate manner). The notification needs to contain specific time frame within the transaction, reported to APMLFT, is supposed to be performed. In the case of temporary notification, compliance officer may deliver the information on suspicious transaction to the APMLFT in electronic manner (over secure web page of the APMLFT, fax) or over telephone, but it also needs to be delivered in written form, the latest on the following working day.

PROFESSIONAL IMPROVEMENT

The compliance officers department responsible for human resources, in co-operation with compliance officer needs to create the program of professional preparation and improvement in the field of prevention and detection of money laundering and terrorism financing, for each calendar year, the latest till the end of the first quarter of business year. The program needs to contain:

- ✓ Content and scope of educational program,
- ✓ The goal of educational program,
- ✓ The manner or accomplishing educational program (teaching, workshops, practices etc.),
- ✓ Group of employees the program is dedicated at,
- ✓ Duration of educational program.

APPLICATION

These Guidelines are enforced on the day of signing and would be applied from 25, September 2009.

Number:
Podgorica, 14, September 2009.

6. Rulebook on Indicators for recognising suspicious customers and transactions

In accordance with the article 46 of the on the Prevention of Money Laundering and Terrorist Financing ("Official Gazette of the Republic of Montenegro ", No. 14/07), The Ministry of Finance adopted

Article 1
The list of indicators for recognising suspicious customers and transactions is closely defined by this Rulebook.

Article 2
The list of indicators for recognising suspicious customers and transactions is printed together with this rulebook and it makes the integral part of it, as follows:
- List of Indicators for banks,
- List of Indicators for capital market,
- List of Indicators for the Customs Administration,
- List of Indicators for the Department of Public Revenues,
- List of Indicators for leasing companies,
- List of Indicators for auditors,
- List of Indicators for accountants,
- List of Indicators for lawyers and
- General indicators.

Article 3
This Rule book shall come into force on the 8th day after it is published in the "Official Gazette of the Republic of Montenegro" ".
No : 02-
Podgorica, 7th October 2009
Minister of Finance
dr Igor Lukšić

LIST OF INDICATORS FOR BANKS

CASH TRANSACTIONS

1. Depositing or converting into another currency large amounts of small denomination bills into large denomination bills especially if it is outside of the normal course of business of the customer.
2. Frequent payments or numerous bank notes that are battered or damaged.
3. Single payment of a large sum of money on an account of an natural person that is automatically withdrawn from the account.
4. Multiple deposits of small amounts on an account of an individual which are transferred to one account
5. Paying taxes with large amounts of cash..
6. Repeated (consecutive) conversions of large amounts of money into foreign currency.
7. Purchasing financial instruments (securities, insurance policies) in large amounts for cash.
8. Customer conducts cash transactions which are slightly below the legally determined maximum in order to avoid the reporting requirement.
9. Customer conducts transactions which are unusual for him. .

10. Transaction involves non-profit or humanitarian organisations without an obvious economic purpose, or where there is no logical relation between the purpose of the organisation and other entities involved in the transaction.

UNUSUAL CHANGES ON THE ACCOUNTS

11. Opening accounts for which the signature authority is given to persons that have signature authority in several companies, especially if the companies are related
12. Opening accounts with the signature authority given to the persons that are neither family nor business related.
13. Opening accounts of legal entities on which deposits are made that are not in accordance with the scope of business of the customer
14. Transactions that are not economically justified.
15. Transactions related to payment operations in the country and abroad that are outside normal activities of the customer with regard to the goods, amounts, business partners, scope of turnover, etc.
16. Frequent advance payments
17. Providing illogical information on the transaction to bank officials.
18. Frequent ordering of traveller's checks, frequent issuing of letters of credit for large sums of money.
19. Short term inflows of a large sum of money on an account of the customer that has been inactive for a long time or payment on an account in an off-shore region
20. Multiply transactions carried out by several different persons to one account and without the clear purpose.
21. Flow of large sums of money from one account to another within a closed group of people
22. Attempt to open an account under a false name.
23. Accounts on which several small sums of money are deposited and there is one time withdrawal of a large sum..
24. Transactions involving several accounts, some of which become inactive for a long time.
25. Depositing a higher amount of cash as deposit for the purpose of obtaining credit, and afterwards an unexpected request form a customer to pay of the credit before the deadline
26. Customer deposits considerable amounts on an account and gives an order to a bank for the amounts to be transferred on the accounts of a great number of persons, especially in cases when there is no rational explanation or economic justification for such transactions
27. Frequent transfers to huge and rounded amounts.
28. Frequent transactions on the basis of advance payments or advance returns that are substantiated by a customer with the non- execution of commercial contracts.
29. Transfers of huge amounts in foreign countries from the account of a customer when the account balance originates from numerous cash deposits on different accounts of customers at one or more banks.
30. Small enterprise operating on only one location performs transactions of depositing or withdrawing funds in more branches of the same bank, which could be evaluated as impractical for that enterprise.
31. Considerable increase of the amount, or frequency of cash deposits or withdrawals from the account of an enterprise whose activity is providing professional and consulting services, especially when the deposited funds are immediately transferred on other accounts.
32. Transactions between private and business account of an enterprise, which do not indicate to a clear economic justification.
33. Transactions including withdrawal of funds soon after the funds have been deposited at reporting entity (only through an account), when this rapid withdrawal of funds is not justified in the business activity of a customer.

34. Unexpected/ sudden paying off a debt without a convincing explanation.
35. Loans granted by off-shore companies.
36. Unexplained electronic transfers of funds by a customer.
37. Accounts are used for receiving or paying of huge amounts, but they do not show so called normal activities related to the operating, such as, for example, payment of salaries, paying bills etc.
38. Transactions with a country that is considered as non-cooperative by Financial Action Task Force (FATF) or business relationships with customers whose permanent residence is in such countries.
39. Issuing payable guarantees by a third party unknown to the financial institution, which do not have a clear relationship with a customer or a good reason for offering such guarantees.
40. Transfers of huge amounts of money with instructions to pay of the funds to the beneficiary in cash.
41. A great number of different individuals paying in deposits on the same account number.
42. Depositing or payment of the higher amounts of the effective money (in Euro currency or other foreign currency) which significantly differ from the customer's usual transactions because they are not in accordance with incomes or customer's status, particularly if the transactions are not typical for the business activities of a customer.
43. Considerable increase of the amount, or frequency of cash deposits or withdrawals from the account of an enterprise whose activity is providing professional and consulting services, especially when the deposited funds are immediately transferred on other accounts
44. Trade or conversion of numerous traveller check's or securities for cash, especially if those transactions are not typical for a customer.
45. Frequent transactions based on the or return of advance which customer explains with non completed contracts.
46. Customer carries out transactions that include several intermediaries or accounts, especially if the customers who are carrying out those transactions are citizens of countries that do not apply regulations from the prevention of money laundering area or where very rigid laws on bank and business data secrecy are in force.
47. Transactions that are recognised as suspicious by employees with the bank, in accordance with their experience and knowledge.
48. Safe deposit box is only used by a person defined as an authorised person in the leasing contract and this person requires cancelling of the safe deposit box leasing contract.
49. Frequent remittance, domestic and foreign, in smaller amounts and ongoing- connected transactions, with the purpose of concealing the real amount of assets in transaction.
50. There are no evidence on transactions (data on sender), or provided evidence for transaction does not correspond to the swift message and other data for payment (contract, invoice, preliminary calculation,, annexes to a contract etc..
51. Politically exposed persons are carrying out transactions with countries which are is recognised as non cooperative by Financial Action Task Force (FATF), or establishing business relationships with clients whose place of residence is in these countries.

BEHAVIOUR OF CUSTOMERS AND EMPLOYEES

52. Customers open accounts or conduct transactions in the branch offices which are not economically or geographically justified
53. Customers conduct transactions through several accounts in several branch offices without the real economic or other reason.
54. Customers are nervous. They avoid answering questions related to the transactions. They assume a defensive posture. They are reluctant to provide identification. They provide false documents or data.

55. Transactions with large amounts of money conducted by public officials, clerks or employees or political exposed persons that are not in accordance with their income or position.

56. Customer asks for assistance to complete the documents while opening an account or he can not provide the necessary information.
57. Customer does not know or is unable or unwilling to provide information concerning the nature of the business or about the owners of the firm.
58. Documents do not show clearly the identity of owners and/or authorised persons to represent the firm.
59. Representatives of a business that is registered in territories of so called high risk countries or off-shore regions want to open an account.
60. Founders of the company are identified as suspicious by law enforcement or other sources.
61. There are valid reasons to believe that the submitted documents to open an account are forged or their authenticity can not be verified.
62. Customer insists that a transaction is conducted promptly.
63. Customer offers statements that the money is clean and that it is not laundered without being questioned in this regard.
64. Customer refuses to show personal documents
65. Customer asks questions about certain facts, which point to his desire to avoid the reporting requirement.
66. Customer shows only copies of his personal documents.
67. Customer attempts to prove his identity using some other documents that are not usual personal documents..
68. The customer's documentation does not contain usual data such as phone number and address etc
69. The customer's personal documents are new and recently issued.
70. Customer has never been employed, and owns considerable funds on the accounts.
71. Customer holds open accounts in few branches of the same bank, deposits cash on each of them, and the sum of payments is a considerable one.
72. Customer often deposits funds for which he/she states that they originate from asset sale, while the existence of the asset is questioned.
73. Authorised persons for disposing of the funds on the account of an enterprise refuse to provide complete data on business of the enterprise.
74. Customer makes cash deposits on the account of his/her enterprise with the purpose of paying for "founder's loan" or "increase of founder's deposit".
75. Customer withdraws high sums of money from the account on which significant funds have been transferred on the basis of a credit granted from a country that does not implement the regulations from the prevention of money laundering area.
76. Customer transfers funds on the account in a country his/her enterprise has not had business relationship or receives remittances from business entities he/she had no connections and previous transfers
77. Orderer or the user/beneficiary of the remittance is the citizen of the country that does not apply regulations from the prevention of money laundering area, or which is on the consolidated list of the Sanctions Committee on the basis of UN Security Council Resolution 1267.
78. Customer carries out transactions with persons or companies registered in the countries known as narco-countries and through whose territory narcotics are distributed, or where very rigid laws on bank and business data secrecy are in force.
79. Customer – a legal person, submits a loan application, despite the fact that the economic and financial standing indicators do not imply the customer's need for a loan. The funds from the loan are afterwards transferred on the accounts in an off-shore bank, or in the favor of a third party, or are used without clear purpose.

80. When carrying out a transaction, a customer is supervised by a third person.
81. Customer frequently deposits or withdraws funds in the amounts that are somewhat lower than the threshold required for identifying and reporting.
82. Customer requires the business relationship to be terminated and to establish a new relationship with a bank in his own name, or in the name of a family member, with no documented traces left.
83. Customer frequently (in a short period of time) via cash dispensers withdraws cash in the amounts that are under the threshold required for identifying and reporting.
84. Customer carries out transactions in high amounts and through an account that has been inactive for a long period of time and possibly gives order for closing an account.
85. Customer frequently deposing assets, claiming that it derives from property sale while the existence of this property is disputable.
86. Customer has unusually good knowledge of legal provisions related to the prevention of money laundering and terrorist financing and reporting suspicious transactions, very "gabby" in relation with topics referring to money laundering and activities of terrorist financing, rapidly confirms that the assets at his/her disposal are "clean" and not laundered.
87. Politically exposed persons frequently depositing cash (in high amounts), and the origin of money is not known or can not be established.
88. Natural person issues order to a bank to transfer assets to a third person without evidences on the purpose and intention of this transfer.
89. Customer opens account as natural person or he/she is an authorised person of a legal person but provides personal documentation issued in countries where dual documentation is still valid (states which do not exist but documents they have issued are still valid) and now he appears as non resident.

ELECTRONIC FUNDS TRANSFER

1. Customer transfers large amounts of money abroad with cash payment order to the foreign entity.
2. Customer receives large amounts of money, from foreign locations, that contains cash payment orders.
3. The amount of electronically transferred assets is out of usual business transactions of that customer.
4. Customer carries out fund transfer towards counties known for drugs production and export .
5. Customer carries out transactions within countries known for high level of bank and business secrecy, except when there is about countries that have accepted international standards on prevention of money laundering.
6. Customer carries out electronic fund transfer in/from free or off shore zone, even if this activity is not usual for customer's business activities.
7. Customer carries out fund transfers (in/from) and as a purpose for transaction states different derivative financial instruments (options, futures…)

LIST OF INDICATORS FOR CAPITAL MARKET

INDICATORS OF SUSPICIOUS TRANSACTIONS AT THE STOCK EXCHANGE BUSINESS

WHILE OPENING AN ACCOUNT

1. When a customer expresses unusual request for the privacy protection, especially with regard to the data related to his identity, type of industry, assets or business.
2. When a customer refuses or avoids showing the origin of funds for each transaction with the value exceeding 15.000 Euros or when there are grounds for suspicion that the funds were gained from illegal sources.
3. When an employee estimates that a customer broke a transaction into several separate transactions in order to avoid identification.
4. When a customer pulls from giving a payment order in order to avoid identification after he has been told in accordance with the law provisions that his identity should be checked.
5. When a customer is not interested in the commission, other expenses and the risks to the transaction.
6. When a customer conducts a transaction as an authorised person and he does not want to identify the entity in the name of which he conducts the transaction, especially if the entity resides and has the main office out of the Republic of Montenegro territory.
7. When a customer cannot explain the nature of his business industry.
8. When a customer has several accounts under the same name, or several sub accounts under different names for no particular reason.
9. When a customer is from or has an account in the country, which has been identified as a risk country, because it does not apply the standards in the area of the detection and the prevention of money laundering.
10. When a customer has been convicted for the criminal offenses involving the payment operations, the economic activities and discharging official duties.

WITH REGARD TO CONDUCTING THE TRANSACTION

11. The transaction a customer wants to conduct is not in accordance with his financial status or the course of business.
12. Customer shows interest in purchasing securities for large amounts without special analysis or broker's or investment manager's advice, and such a transaction does not have a clear financial purpose.
13. The transaction a customer wants to conduct is not of a kind that he would be expected to conduct, because the transaction has unclear purpose and is conducted under unusual circumstances.
14. Customer purchases securities from numerous accounts in the banks
where he previously deposited cash, especially if the funds were deposited in amounts which are slightly under the reporting threshold.
15. Customer conducts transfers of monetary funds or securities from one account to other account, none of which is connected to the customer.
16. Customer's account shows sudden inflow of monetary funds, especially if the customer's account has previously been inactive, or deposits are not in accordance with his financial status.
17. Customer's account shows inflow of monetary funds from the accounts in the countries which are risky because they do not apply standards in the area of the detection and the prevention of money laundering.

18. Customer's account shows major inflow of monetary funds while the securities account does not undergo any changes.
19. Customer attempts to create an image of real trade in securities, but instead he conducts fictitious or simulated trade in securities.
20. The proposed transaction is financed by the international wire transfer of money, especially from the countries without an efficient anti-money laundering system.
21. Announced block trade in shares at price slower than the market ones, when buyers are unknown or newly formed companies, and particularly the companies registered on offshore territories.
22. Customer invests in prime and very promising shares, without expressing an interest in the results, or suddenly and without purpose sells the shares.
23. Customer often changes brokerage houses in an effort to conceal the scope of his/her business and the financial standing.
24. Trades and transactions carried on through a brokerage-dealer house that has previously been punished by the Securities Commission for irregular or undue carrying on business.
25. Trade in securities with a planned loss, when a customer frequently purchases securities and soon after sells them below cost.
26. Trade in shares that have been the subject of collateral on the basis of granted loans to the share owners.
27. Customer has poor reputation; he/she is known for illegal activities from the past or connections with persons related to illegal activities.

INDICATORS OF SUSPICIOUS TRANSACTIONS FOR CUSTOMS ADMINISTRATION

IMPORTER/EXPORTER/GOODS

1. The business has previously committed Customs violation.
2. The business was founded recently and conducted substantial import/export operations over a short period of time.
3. The business uses services of a suspicious shipping or transport company.
4. The business is known to have financial problems.
5. The business is not specialized for trade but only occasionally conducts trading.
6. The business that is specialized in importing or exporting products from certain countries changes the source of procurement or destination of his products.
7. The business chooses to change location of the Customs examination.
8. Goods are imported from a country known as the source or transit country for narcotics.
9. The business is not registered in the Customs register.
10. Goods are imported or exported in an usual or indirect manner.
11. The value of goods are similar to or lower that the transport costs?
12. The number of the seal does not agree with the number written in the customs documentation.
13. The seals are either impossible to identify or they are perfectly clear.

TRAVELLER / VEHICLE

1. There is a failure to properly declare currency or goods to Customs authorities in accordance with the law.
2. The appearance of the traveler is not in accordance with the purpose of the stated travel.
3. If traveling by public conveyance there is a one way ticket.
4. Traveler is using a leased vehicle.

5. Driver is extremely cooperative or offers information without being asked.
6. The traveler's passport has recently been issued.
7. The traveler always uses the same flight or schedule.
8. The traveler gives a vague or incomplete explanation of the purpose of the travel and the date of return?
9. The travel destination is known for being a source location for narcotics or other illegal activities.
10. There any indication of modification remodeling or changes to the vehicle that may signal secret compartments.

INDICATORS OF SUSPICIOUS TRANSACTIONS FOR THE TAX ADMINISTRATION

CASH CONTRARY TO REALISATION

1. It is used in accounting for large enterprises while selling goods (services). Transaction is usually conducted, turnover is reported even if no payment was made at all. The same pattern is used for business expenditures. Activities with legal appearance through which cash could be sent to the business account are for example: food market business, restaurants and hotels, bars, night clubs, etc. For example, it also happens that individual payments of daily earnings are conducted even when the industry is not performed.

KEEPING RECORDS ON SUPPLIES

2. Accounting on cash is usually combined with supplies. Keeping records on supplies belongs to the system based on realisation. Each abnormal increase or drop of figures related to the supplies should be examined.

BALANCE SHEET (ASSETS, FUNDS, LIABILITIES AND CAPITAL)

3. Balance sheet represents the reflection of the value of the capital that is engaged in certain business, loans, as well as data as to who the creditors are, retained profit that represents business pre-history of the company, assets engaged in that business, etc. It should be determined who participates in the ownership and loans. There is always suspicion in case the balance sheet is not in accordance with the tax returns.

METHODS OF LIVING COSTS AND THE METHOD ON NET VALUE AND DEPOSITS IN THE BANKS

4. How much money does the taxpayer spend, where did he earn the money and what does he do for living? If he cannot prove that the assets were paid from the business revenues, then there are other sources of funds. If the total bank deposits exceed the reported turnover and the taxpayer cannot prove where the money came from, the reason to conduct examination appears immediately. In general, whenever the source of funds cannot be proved the examination should be conducted.

CASH

5.Turnover gained in cash has tendency to be used for the new investments, or for personal needs, and the next step would be to send the money back to a firm from which it can be used without raising suspicion, i.e. that the source of money can be explained easily.

RECEIVABLES

6. Balance due, especially a large one, should be examined. This refers particularly to the buyers that are not related to certain business. This usually reveals some private activities that have been conducted through that business.

LIABILITIES TO CREDITORS AND SUPPLIERS
7. Loan given by a shareholder to a firm is shown as payable loan. It is always suspicious when capitalized firms, which have inappropriate status of basic funds according to the balance sheet, convert loans into share capital.

EXAMINING TURNOVER ON THE ACCOUNT
8. Was cash recorded in the turnover and was cash deposited in the banks together with the checks? If not, check the account in the banks due to potential unusual transactions, check the goods that was taken for personal use and whether those amounts were included in the total turnover.

BAD DEBT
9. Examine major and unusual items in the accounts (write-off) and check whether they were previously reported as revenues. In case of writing off from the account of a shareholder, taxpayer or foreigner that is subject to examination, examination should be obligatory.

TRAVEL EXPENSES AND ENTERTAINMENT EXPENSES
10. Are they business oriented or in favor of a shareholder or an employee? Are expenses for purchasing luxurious commodities related to business needs or in favor of the owner?

TRANSACTIONS WITH CONNECTED PERSONS
11. Compulsory examination, especially with large firms that have their own accessory companies located in foreign countries. Also, if the funds are obliged to be transferred to other persons, it is particularly important to examine firms whose the owners of which are both directors or clerks, because there are transactions between two parties (owner and firm) and it should be examined whether they are treated in accordance with «arms length transactions« i.e., under the reasonable conditions as if the parties involved in the transaction are not connected at all.

INDUSTRY MARGINS
12. Use of substantially lower or substantially higher margin than normal for the industry.

HIGH RISK LEGAL ACTIVITIES (RELATED TO THE BANKS – CONTRACTS ON FORFEITING, FACTORING, ETC.) AND THE FINANCIAL DERIVATIVES (FUTURES, OPTIONS AND SIMILAR CONTRACTS)
13. High Risk activities are included in the list because the bank with claims enters into the risky situation while collecting debt from the third person (person liable to perform the obligation assigned) – forfeiting, or the firm in case of factoring. Payment of claims does not depend on the bank or the firm, but on an uncertain event that was not known when the contract was signed. They are used mostly while delivering equipment (export) or constructing a building, so called “turn key” operations.

INDICATORS LIST FOR LEASING COMPANIES

1. Customer submits request for approving financial leasing and given data are incomplete or incorrect with obvious intent to conceal the basic information related to identity of customer or its business activity
2. Transactions for which directors or owners of legal persons, or persons on whose behalf the transaction was carried out, never appears in person not even to sign the contract on financial leasing but instead of them this is done by other persons possessing a special (ad hoc) authorisation. All this is activities are performed with excuse that can not be checked (illness, unspecific obligations etc.) or give authorisation to the third persons in order to avoid direct contact with employees with the leasing companies.
3. A request for financial leasing which seems unjustifiable due to the purpose of equipment or in relation to the business activity of a customer (for example: obvious disproportion between the size of investment and type of business of leasing receiver or in case when the equipment that is purchased by the contract on leasing is not appropriate to customer's business activity or to business activity which the customer plans to perform).
4. Distributor of the leased equipment performs partial delivery
In order to avoid the amount of transaction that is subject to report that must be delivered to APMLTF . In case when distributor, in co-operation with the receiver of leased equipment, delivers equipment through few leasing companies, in the aim of removing the risk it is important to establish the following: that the delivered equipment is completed or that delivered goods is supplement of the previously imported equipment which the receiver already uses (for example: spare parts for current maintenance).
5. Equipment leasing Business when the equipment is offered for price that significantly differs from the real market price.
6. Distributor of the leased equipment neither is the manufacturer nor it is known as seller of goods or equipment that is the subject of leasing.
7. Leasing business of second hand equipment that is not connected with the regular business activity of leasing equipment distributor and distributor is not involved in selling this type of equipment (neither new nor second hand equipment)
8. Leasing business for which the third party provides guarantees (assurance, mortgage, deposit etc. sl.) and when the connection between leasing user and the person offering guarantees is not clear as well as the reasons why the guarantee is offered to the leasing user.
9. Leasing business in which there is a provision on repurchasing leased equipment by distributor and it is offered by distributor spontaneously and under non-market conditions, and specially when distributor of leased equipment is not familiar to the leasing company.
10. Receiver or distributor of leased equipment unwillingly provides information on itself, its business activities or business relations with other leasing companies, especially when concealment of these information disables access to better conditions for concluding leasing business.
11. Customer with no justifiable reason communicates with leasing companies or its subsidiaries that are away from the company's register office.
12. Customer, with no real reason, performs payment form another subsidiary /the account different than the account defined in the original contract.
13. Customer submits request for approving leasing on the basis of guarantees issued or for which asset cover is provided by bank of suspicious solvency, bank from off shore country. Bank from a country through which drug trafficking is caring out or bank from a country where regulations on the prevention of money laundering and terrorist financing are not applied .
14. Customer offers, with no justifiable reasons, offers participation in leasing business and it is significantly higher than the amount that is usual at the leasing market.

15. Customers that are carrying out leasing business with cash payments or checks rather than transactions through the bank account
16. Customer pays its debt by a leasing contract with assets transferred form abroad and from accounts opened in banks situated in countries where the standards on the PML/TF are not implemented or from countries where the strict regulations on bank and business data secrecy and confidentiality are in force.
17. Customer deposits high amounts of cash as participation for getting leasing and afterwards unexpectedly pays off the rest of its debt before the payment deadline.
18. Customer signs the contract on financial leasing accompanied by a person that obviously supervises customer's behavior or insists that the business should be done quickly.
19. Customer provides only copies of documents that are necessary for customer's personal identification or documents issued abroad and its authenticity can not be easily confirmed due to justifiable reasons.
20. Customer possess unusually good knowledge on regulations related to PML/TF and reporting suspicious transactions, customer is very talkative in relations to the topics on money laundering and financing terrorist activities and confirms quickly that his/her assets are "clean" and that they are not "laundered" .

INDICATORS LIST FOR AUDITORS

1. Customer is not familiar with its business and it can be concluded that the customer does not performs its business at all or performs it in very limited range.
2. An Auditor is not allowed to check business premises or production facilities of a customer and it can be concluded that the company is fictitious
3. Complicated organisational structure of the corporation which, in relation to its business activity, is not efficient and due to that it ins not economically justifiable
4. A legal person is established with no particular or justifiable business reason.
5. An orderer pays in advance for the business that has not been contracted yet, and it is less likely that it will be realised.
6. High, unclear oscillations in incomes or unusually higher incomes than business expenditures.
7. Customer, contrary to its business practice, requires from an auditor to perform, on his/her name and account, a transaction for a customer
8. Unusual transactions, most often with connected persons or persons that are different than usual customers (for example: payments to natural persons).
9. There are no evidences on transactions (information, clarifications), or those evidences are not satisfactory.
10. Booking transactions on the basis of unauthentic and incomplete documentation
11. Transactions with legal persons in which identity of beneficiary owner is difficult to establish.
12. Cash based business mainly appears at the legal person that conducts business activity for which cash payment is unusual type of realisation of business transaction
13. Payment for undefined actions or payments that differ from usual payments.
14. Enormous delay when opening account of legal person (account of legal person is opened much later that the time when legal person was established)
15. A legal person is founded without economic reason
16. Often trips abroad that are, with the view to business activities of the legal person, unnecessary or to be more precise unusual
17. Legal person possess several recorded individual transactions that are, with the view on other transactions, unusually high.
18. Executing cash transactions below the threshold for which an identification is prescribed. .

19. Cash business is mostly performed below the threshold for which an obligation to be reported to the Administration is prescribed.
20. Concluding contracts on life insurance, with one shot premium, and early termination of contract without justifiable reason
21. Opening numerous accounts without clear economic- legal justifiability and business activities are done through these accounts, contrary to the regulations, they are not presented in balances.
22. Conducting business activities with entities from countries through whose territory narcotics are distributed, or that do not apply regulations from the prevention of money laundering and terrorist financing area .

LIST OF INDICATORS FOR ACCOUNTANTS

LIST OF INDICATORS FOR RECOGNISING SUSPICIOUS TRANSACTIONS FOR LEGAL AND NATURAL PERSONS THAT PROVIDES AUDITING SERVICES

1. Customer performs recapitalization of the legal entity without economically justifiable reason .
2. Customer, without established reason, does not open business account not even after one year from the date of registration into the Central Register of Commercial Court and it is known that this legal entity performs business activities.
3.Customer, without economical or legal justification, opens or has numerous accounts, or performs business activities through those accounts that are not, contrary to regulations, presented at the balance.
4. Customer does not possess records of regularly employed persons or contracted employees what is unusual for business activity which that legal person performs.
5. Customer is not sure where its business documentation is stored.
6.Customer often and with no basic reason, changes person(s),that for him/her conduct auditing.
7. Customer, contrary to business practice, requires from accountant to perform, on his/her name and account, a transaction for a customer .
8. Termination of the contract on co-operation due to requirements for additional explanation of realisation(or announcement of realisation) of certain transactions, without any established reasons.
9. High, unclear oscillations in incomes or unusually higher incomes than business expenditures
10. Insufficiently explained short term income, that is in the amount 10 times higher than average monthly realisation in the previous year, for the same business activity, and it is done without increase in the scope of business activities.
11. Debt and obligation write offs that amount 10% of customer's assets.
12. Customer's Business activities with entities from countries through whose territory narcotics are distributed, or that do not apply regulations from the prevention of money laundering and terrorist financing area ..
13. Customer's Business activities with entities from countries that are known as "tax paradises" (for example: payment for consulting services or payments for examining entities that do not conduct trade or production activities in the state where they are registered)
14. Inflows from foreign accounts or outflows to foreign accounts where customer does not have any business partners.
15. Frequent, illogic payments to daughter company or different connected companies or payments to natural persons.
16. Executing cash transactions below the threshold for which an identification is prescribed .
17. Cash based business is mostly performed below the threshold for which an obligation to be reported to the Administration is prescribed

18. Early cash repayments of credits or loans .
19. providing loans for shareholders or employees and that is contrary to regulations
20. Payments for undefined services .
21. Concluding contracts on life insurance, with one shot premium, and early termination of contract without justifiable reason
22. There are no clear evidences on transactions or transactions are executed without a clear purpose.
23. Increase of share capital for companies without additional registration at Central Register of the Commercial Court.
24. Customer, user of auditing services, conducts business activities that include significant number of cash transactions or cash amounts.
25. Customer, user of auditing services, uses complex structure without obvious business or any other reason, especially when the beneficiary owner of the company can not be established.
26. Customer, user of auditing services, has its registered offices or performs high risk business activities or business activities in high risk countries.

LIST OF INDICATORS FOR LAWYERS

General data on customer, its documents and intentions
1. Customer avoids the meeting and identification in person breach the business relationship with a lawyer when he/she becomes informed on identification obligation
2. Customer breaches business relationship by authorisation(since he/she is authorised representative) because of the request for additional explanations or additional documentation, without obvious reasons
3. Customer's phone is turned off or it is established that customer's number does not exist at all .
4. Customer uses fictitious name or address
5. Customer possess unusually good knowledge on regulations related to reporting suspicious transactions, and confirms quickly that his/her assets are "clean"
6. Customer unwillingly provides information on itself, its business activities or business relations with other persons (legal or natural), especially when concealment of these information disables access to better conditions for concluding specific contracts.
7. Customer provides only copies of documents that are necessary for customer's personal identification or documents issued abroad and its authenticity can not be easily confirmed due to justifiable reasons.
8.Customer offers much more money for the service that is provided to him/her than it is usual for that kind of business.
9. Customer requires advise on conducting specific legal business that is connected with criminal act. Criminal
10. Customer is a citizen of country through whose territory narcotics are distributed, or its registered office, or address, is in a country that does not apply regulations from the prevention of money laundering and terrorist financing area .

REAL ESTATE TRADE

11. Customer sold a real estate within a relatively short period even if in the process of sale it is obvious that this sale will be a business loss for customer.
12.Customer,in a short period, conducts numerous purchases without any economically or legally justifiable reasons.

13. Customer requires conducting trade contracts in high amounts (where the customer appears as buyer) and after realisation of the first part of contracted business transaction, aborts trade, specifically requires breach of the contract even if it is known that the customer possess enough financial assets for realisation of the trade contract. Customer consciously losses certain financial assets, without any economically or legally justifiable reasons, by this act.
14. The pre-contract requires from lawyer stating disproportionately higher prices than market prices
Disposing customer's money – securities or other property. Disposing customer's bank account, savings or share trading account
15. In the process of planning transaction, customer plans to make deposits at numerous accounts, (with the same bank but different subsidiaries or different banks), and than the total amount of payments, that is a significant sum, to transfer in countries that do not apply regulations from the prevention of money laundering and terrorist financing area .
16. Transactions with country that is designated by Financial Action Task Force (FATF) as non-cooperative or business relationships are established with entities whose place of residence is in the mentioned countries.
17. Frequent unusual transactions, often with persons that differ from regular customers.
18. Customer's Business activities are performed with entities from countries that are known as "tax paradises" (for example: payment for consulting services or payments for examining entities that do not conduct trade or production activities in the state where they are registered)
19. Customer, contrary to business practice, requires from lawyer to perform, on his/her name and account, a transaction for a customer
20. There are no clear evidences on transactions or transactions are executed without a clear purpose.

GENERAL INDICATORS

1. Customer brings high amount of cash and intend to execute a transaction.
2. Customer's business transactions are not in accordance with customer's known income or position.
3. Customer provides unclear explanation on its source of incomes or cash which he/she uses in business transactions.
4. Customer claims or states that the origin of incomes or cash is illegal
5. There are data that customer is allegedly involved in for illegal activities .
6. Customer requires to pay in installments in order to avoid cash payment in the amounts which are slightly under the reporting threshold.
7. Customer requires that the report on cash transaction should not be composed or rejects to execute transaction after receiving information that there is reporting obligation. .
8. Transaction that customer executes is not in accordance with his/hers usual business practice.
9. Customer intends to buy property or conduct business on behalf of another person for example: acquaintance or cousin (besides its suppose).
10. Customer does not want that his/her name is recorded in any document that could connect him/her in relation with the certain business transaction.
11. Customer provides inadequate explanation why does he/she, in the last moment, changes names of persons that are used in relation with the transaction.
12. Customer negotiates on performing business by market price or price higher than required but demands that lower price should be provided in the documents, and he/she is paying price difference underhand
13. Customer pays advance in a high amount of cash, while the rest of it is financed from an unusual source or offshore bank.
14. Customer buys property, especially real estates, blindly (without seeing or checking it).

15. Customer buys property or invests in real-estate business in a short term period and acts as very interested in location, status or projected expenses for repairing the property.
16. Customer performs real-estate business (buying, selling, replacing) in cash and for the benefit of himself/herself, members of its family and third persons, in the amounts exceeding 150.000 €.
17. Customer would like to know more about unusual ways of .
18. Customer does not want to identify itself in case of real-estate trade in cash or identifies itself with counterfeited data or documents.
19. Customer that is known from the public life, buys real estates in high amounts and the value of the bought property differ from his/her income status.
20. Customer that purchases real estates is a young person and it is obvious that this customer disposes luxurious status symbols (expensive automobiles, motorcycles, vehicles, watches etc.).
21. Customers that are residents or non residents purchase real-estates for domestic legal person even if it is obvious that the purpose of real-estate trade is purchasing real-estate for non resident natural person.
22. Customer natural or legal person asks or executes transactions on real estate for natural or legal persons, residents or non residents, that are from off shore destinations or for off shore companies and also from countries known for narcotics distribution and production narcotics or countries that do not apply regulations from the prevention of money laundering and terrorist financing area .
23. Payments of high amount insurance premiums.
24. The insurance user requires cash payment for money form insurance or return of insurance premium in case that there is a high amount of money.
25. High insurance amounts for number of insurance policies, that are concluded in short time period, are paid in cash.
26. It is suspected that insurance policies are concluded on fictitious names, names of other persons or fictitious addresses.
27. One person owns numerous insurance policies issued at different insurance companies, especially if insurance contracts were concluded in a short time period.
28. Insurance policy owner makes changes at insurance contract and requires insurance policy with higher premium or to change monthly policy payments to annual policy payments or insurance at fixed premium, and it is not in accordance with its income status.
29. Cancelling insurance policy soon after concluding insurance policy contract soon after concluding insurance policy contract, especially when there is large amount premium.
30. Customer demands compensation from insurance, money that is demanded on the basis of compensation in case of cancellation of policy or overpaid amount of insurance premium to be paid off to a third party or transferred to the account of natural or legal person on the territory of the state where are applied high standards in the area of money laundering and in which are prescribed strict regulations on confidentiality and secrecy of bank and business data.
31. Customer accepts unfavorable terms of insurance contract, with regard to his health condition and age.
32. Companies that are owners of insurance policies pay on behalf of their employees unusually large insurance premiums or cancel policies in very short time period from the date of concluding insurance contract
33. Companies purchase insurance policies for their employees, and number of employees is lower than number of purchased policies: polices are issued even for persons that are not employed in company.
34. Insurance contract is concluded by person who carried out illegal activities in past or insurance contract is concluded by person that in some manner can be connected with these activities.
35. Contractor insurance or the insured insists on transaction secrecy, i.e. not to report the amount of the insurance premium or the amount of the insurance to the APML despite the fact that it is a

statutory obligation of the insurer. A customer attempts, by plead or bribe, to convince the employees in the insurance company to represent his/her interests which is against the law.

6. EXTRACTS FROM THE CRIMINAL PROCEDURE CODE OF MONTENEGRO (Official Gazette of Montenegro, no. 57/09, August 18, 2009)

Provisional Seizure of Property Gain and Financial Investigation for the Purpose of Extended Seizure of Property
Article 90

(1) In the procedure conducted for the criminal offence for which the Criminal Code provides for a possibility of extended seizure of property from the sentenced persons, their legal successors or persons to whom the sentenced persons have transferred their property who are not able to prove the legality of its origin, and grounds of suspicion exist that the property in question was illicitly acquired, the court may, at the proposal of a State Prosecutor, order the property to be provisionally seized.
(2) The State Prosecutor shall initiate a financial investigation by way of an order against the suspects or accused persons for the criminal offence referred to in paragraph 1 of this Article, their legal successors or persons to whom the suspects or accused persons have transfered certain property.
(3) During the financial investigation, evidence shall be collected on the property and revenues of suspects or accused persons, their legal successors or persons to whom the accused persons have transferred property that was acquired in the period prescribed by the Criminal Code.
(4) In the procedure of provisional seizure of property referred to in paragraph 1 of this Article, provisions of the law regulating enforcement proceedings shall be applied accordingly, if provisions of the present Code do not prescribe otherwise.

Criminal Offences for Which Measures of Secret Surveillance May Be Ordered
Article 158

The measures referred to in Article 157 of the present Code may be ordered for the following criminal offences:
1) for which a prison sentence of ten years or a more severe penalty may be imposed;
2) having elements of organised crime;
3) having elements of corruption, as follows: money laundering, causing false bankruptcy, abuse of assessment, passive bribery, active bribery, disclosure of an official secret, trading in influence, as well as abuse of authority in economy, abuse of an official position and fraud in the conduct of an official duty with prescribed imprisonment sentence of eight years or a more serious sentence.
4) abduction, extortion, blackmail, meditation in prostitution, displaying pornographic material, usury, tax and contributions evasion, smuggling, unlawful processing, disposal and storing of dangerous substances, attack on a person acting in an official capacity during performance on an official duty, obstruction of evidences, criminal association, unlawful keeping of weapons and explosions, illegal crossing of the state border and smuggling in human beings.
5) against the security of computer data.

Extended Effect of an Appeal
Article 401

An appeal filed in favour of the defendant due to the state of the facts being erroneously or incompletely established or due to the violation of the Criminal Code shall be deemed to contain an appeal against the decision concerning the criminal sanction and forfeiture of the property gain referred to in Article 389 of the present Code.

Motions to Indict in the Summary Proceedings
Article 447

(1) The criminal proceedings shall be instituted upon the bill of indictment of the State Prosecutor, a subsidiary Prosecutor or upon a private action.
(2) A bill of indictment and a private action shall be submitted in the number of copies as needed for the court and for the accused person.

Detention in the Course of the Summary Proceedings
Article 448

(1) For the purpose of an uninterrupted conduct of the criminal proceedings a detention may be ordered against a person against whom there is a grounded suspicion of having committed an offence if:

1) if s/he is in hiding or his/her identity cannot be established or if there are other circumstances indicating a risk of flight,

2) if special circumstances indicate that s/he shall complete the attempted criminal offence or perpetrate the criminal offence he threatens to commit.

(2) Before a bill of indictment is submitted, a detention may last only for the time necessary to conduct evidentiary actions, but no longer than eight days. The Panel (Article 24, paragraph 7) shall decide on an appeal against a ruling on detention.
(3) From the moment a bill of indictment is submitted until the conclusion of the trial, the provisions of Article 179 of the present Code shall be applied accordingly in respect with detention, and the Panel shall review every month whether the grounds for detention still exist.
(4) When the accused person is in detention, the court shall proceed as expeditiously as possible.

Instituting Prosecution
Article 449

(1) If a criminal charge was submitted by an injured party and the State Prosecutor fails within a term of one month to prefer a motion to indict, or to notify the injured party of the dismissal of the criminal charge, the injured party shall be entitled to institute a prosecution in the capacity of a prosecutor by submitting a bill of indictment to the court.
(2) If in the case defined in paragraph 1 of this Article, the injured party waives the prosecution, or it is considered according to law that the injured party has waived the prosecution, the State Prosecutor may, irrespective of the conditions prescribed for the reopening of the proceedings, reopen the proceedings, if the criminal charge of the injured party has not been dismissed.

3. CONFISCATION OF PROPERTY WHOSE LEGAL ORIGIN HAS NOT BEEN PROVED

Request for Confiscation of Property and Contents of Request
Article 486

(1) After the finality of the judgment finding the accused person guilty of the criminal offence for which the Criminal Code prescribes the possibility of extended confiscation of property from the convicted person, his/her legal successor or the person to whom the convicted person has transferred the property and who cannot prove the legality of its origin, the State Prosecutor shall, at the latest within one year, submit the request for the confiscation of the property of the convicted person, his/her legal successor or a person to whom the convicted person has transferred the property for which there is no evidence on the legality of its origin.
(2) The request from paragraph 1 of this Article shall contain the data on the convicted person, his/her legal successor or the person to whom the convicted person has transferred the

property, indication of property to be confiscated, evidence on the property owned by the convicted person, his/her legal successor or the person to whom the property has been transferred, and on their legal proceeds, as well as circumstances indicating the obvious discrepancy between the total property and the legal proceeds of the convicted person, his/her legal successor and the person to whom the convicted person has transferred the property.
(3) The request from paragraph 1 of this Article shall be served without delay to the convicted person, his/her legal successor or the person to whom the convicted person has transferred the property, along with a warning stating that s/he shall prove the legal origin of the property at the Panel session referred to in Article 24, paragraph 7 of the present Code, as well as that the property will be confiscated if its legal origin has not been proved.

Deciding on the Request for the Confiscation of Property
Article 487

(1) Pursuant to Article 314 of the present Code, the Panel referred to in Article 24, paragraph 7 of the present Code shall decide on the request referred to in Article 486 of the present Code at the session from which the public may be excluded.
(2) The following shall be invited to the Panel session: State Prosecutor, convicted person, his/her legal successor or a person to whom the convicted person has transferred his/her property, and his/her proxy.
(3) If the convicted person, his/her legal successor or the person to whom the convicted person has transferred his/her property does not prove by plausible documents or in absence of plausible documents, in some other manner, the legal origin of the property, the Panel shall issue a ruling on the confiscation of the property.
(4) If the convicted person, his/her legal successor or the person to whom the convicted person has transferred his/her property proves by plausible documents or in some other manner the legality of the property origin or of the part of property, the Panel shall issue a ruling on total or partial dismissal of the request referred to in Article 486, paragraph 1 of the present Code.
(5) The panel referred to in Article 24, paragraph 7 of the present Code shall dismiss the request if it was submitted after the expiry of the deadline referred to in Article 486, paragraph 1 of the present Code.

Contents of the Request on Confiscation of Property
Article 488

(1) The ruling referred to in Article 487, paragraph 3 of the present Code shall contain the data on the convicted person, his/her legal successor or the person to whom the convicted person has transferred his/her property, on the property being confiscated, and the decision on the costs of safekeeping and administration of the provisionally seized property referred to in Article 96 of the present Code. If the confiscation of the property would bring into question the sustenance of the convicted person, his/her legal successor or the person to whom the convicted person has transferred his/her property or the persons who they are legally obliged to support, the ruling shall indicate that a portion of the property is exempted from confiscation.
(2) The ruling on property confiscation shall be delivered to the convicted person, his/her legal successor or the person to whom the convicted person has transferred his/her property, his/her proxy, State Prosecutor, and the state authority which, pursuant to the law, shall administrate the confiscated property.

Appeal against the Ruling on Confiscation of Property
Article 489

(1) Convicted person, his/her legal successor of the person to whom the convicted person has transferred his/her property and his/her proxy may appeal against the ruling referred to in Article 487, paragraph 3 of the present Code within eight days; the State Prosecutor may appeal against the ruling referred to in Article 487, paragraph 4 of the present Code.
(2) An immediately superior court shall decide on the appeal referred to in paragraph 1 of this Article.

7. GUIDELINES ON BANK RISK ANALYSIS AIMED AT PREVENTING MONEY LAUNDERING AND TERRORISM FINANCING

Podgorica, 25.02.2010

Pursuant to Article 17 paragraph 1 of the Central Bank of Montenegro Law (OGM 52/00, 53/00, 47/01, 04/05), and with the meaning of Article 8 paragraph 3 of the Law on Prevention of Money Laundering and Terrorism Financing (OGM 14/07, 04/08) and Article 2 paragraph 1 of the Rulebook on the development of guidelines on risk analysis with a view to preventing money laundering and terrorism financing (OGM 20/09), the Council of the Central Bank of Montenegro, on its session held on 25. February 2010, issued

GUIDELINES

ON BANK RISK ANALYSIS AIMED AT PREVENTING MONEY LAUNDERING AND TERRORISM FINANCING

These guidelines shall determine in detail the criteria for issuing internal act of banks and branches of foreign banks (hereinafter referred to as: banks) on risk analysis aimed at preventing money laundering and terrorism financing.

1. Risk of money laundering and terrorism financing

The risk of money laundering and terrorism financing, with the meaning of Article 5 point 5 of the Law on the Prevention of Money Laundering and Terrorism Financing (hereinafter: the Law), is a risk that a client would use the financial system for money laundering or terrorism financing, i.e. that the business relationship, transaction or a product would be directly or indirectly used for money laundering or terrorism financing.
Money laundering, with the meaning of Article 2 of the Law, is considered especially:

1) exchange or other transfer of money or other property which originates form a crime;
2) obtaining, possession or use of money or other property which originates from a crime;
3) concealing a nature, place of deposit, movement, disposal, ownership or rights regarding money or other property which is the consequence of a crime.

Terrorism financing, with the meaning of Article 3 of the Law, is considered especially:

1) providing or gathering, or an attempt to provide or gather money or other property, directly or indirectly, with a goal or with a consciousness that it would be completely or partially used for implementation of a terrorist act or used by terrorist or a terrorist organisation; 2) instigation or assistance in providing or gathering assets or property from item 1 of this Article.

3. Risk analysis of money laundering and terrorism financing

With the meaning of Article 8 paragraph 1 of the Law, a bank is obliged to create a risk based

approach in order to determine the estimation of risk of a group of clients or a client, business relationship, transaction or a product, in order to prevent usage of its services or products for purpose of money laundering or terrorism financing.
In that sense, the bank is obliged to adopt an **internal act on risk based approach** and to apply the risk based approach.

3.1 Identification of the client

Before establishing the business relationship with its client, the bank is obliged to identify the client. With the meaning of Article 7 of the Law, the identification of the client is the procedure which includes: 1) establishing the identity of a client, or if the identification is previously done, to verify the identity based on reliable, independent and objective sources; 2) gathering information about the client, i.e. if the information are gathered, verifying gathered information based on reliable, independent and objective sources.

3.1.1 Identification and verification of a natural person or an entrepreneur

A bank shall, pursuant to Article 14 of the Law, establish and verify the identify of a client who is a natural person, i.e. its legal representative, entrepreneur, or natural person which performs the activities, by verifying the personal identification document of a client, while the client is present, and gathers the following data: The identity of a client who is a natural person can be also established based on qualified electronic confirmation of a client, issued by a service provider of certification in accordance with the regulations on electronic signature and electronic business.

Client data – natural person	
Client data – natural person	□name; □address of temporary and permanent residence, □date and place of birth □tax file number (hereinafter TFN) of a natural person, i.e. its representative; □number, type and title of a state body which issued the document; □name, address of temporary and permanent residence, date and place of birth of the natural person, who has the access to the safe; □purpose and assumed nature of the business relationship, including the information on activities, i.e. the status of a client (employed, unemployed, student, retired, farmer, etc.); □data of establishing the business relationship, i.e. date and time when that person had access to the safe;
Client data – entrepreneur	□name; □address of temporary and permanent residence; □date and place of birth of the entrepreneur or a natural person who performs the activity, who establishes a business relationship or performs a transaction, i.e. a private person on their behalf the business relationship or transaction is performed, type and title of a state body which issued the document; □company, address and, if given, ID number of the entrepreneur or a natural person which performs the activity;

Data on transaction	□ date and time of transaction; □ the amount and currency of the transaction; □ the purpose of the transaction and name and address of temporary and permanent residence, i.e. company and residence of a person for whom the transaction is intended for;

	the manner how the transaction was made; data on the source of the property and assets, which were or will be the subject of a business relationship or a transaction;
Data related to the person representing the client (legal representative or authorised person)	name and family name, address of temporary and permanent residence, date and year of birth, TFN and number of a personal document and title of the state body which issued the personal document

3.1.2 Establishing and verifying the identity of a client – legal person

With the meaning of Article 15 of the Law, the bank shall establish and verify the identity of a client who is a legal person, i.e. its legal representative, or authorised representative by inspecting the original or a certified copy of a personal document (that cannot be older than three months) from the Central Register of the Commercial Court (hereinafter: CRCC) or other suitable public register, which on behalf of the legal person is submitted by the legal representative.
The bank may also establish and verify the identity of the legal person and gather information referred to in Article 71 paragraph 1 of the Law by verifying the information with the CRCC or other suitable public register. With its regards, the bank shall state the date, time and name of the person who verified the information on the statement from the register. The statement from the register shall be filed in accordance with the provisions of the Law.
If the data required by the Law (Article 71 paragraphs 2, 7, 9, 10, 11, 12, 13 and 14) cannot be determined by inspecting the original or certified copies of personal documents, the missing data shall be gathered directly from the representative or the authorised person.
If the bank, during establishing and verifying the identity of a legal person, is suspicious about the validity of given data or validity of documents and other business documentation used for obtaining data, the bank is obliged to receive a written statement from the representative or authorised person before establishing the business relationship or the transaction.
If the client is a foreign legal person performing activities in Montenegro through a business office, the bank shall determine and verify the identity of a foreign legal person and its business office.
The information that the bank collects about a client who is a legal person, are given in the following table:

	Client data – legal person
Client data	company; address; registered office and ID number of a legal person who establishes the business relationship or performs a transaction, i.e. legal person on whose behalf the business relationship is established or transaction is performed
Data related to establishing a business relationship	date of establishing a business relationship or access to the safe; the purpose and the assumed nature of the business relationship, including the information on client’s activity.

Data related to performed transaction	□date and time of transaction; □the amount and the currency of the transaction; □the purpose of the transaction and name and temporary and permanent residence, i.e. company and residence of a person for whom the transaction is intended for; □the manner how the transaction was made; □data on the source of the property and assets.
Data related to the person represented by the client (legal representative or authorised person)	□name; □temporary and permanent residence; □date and place of birth and TFN of the representative or authorised person who, on behalf of another legal person or other person of a civil law concludes the business relationship or performs a transaction; □number and type of a personal document; □title of the state body that issued the personal document.
Data related to the beneficiary owner	□name; □temporary and permanent residence; □date and place of birth of the real client owner of the legal person, i.e. in the case of Article 19 paragraph 3 item 2 of the Law, data about the category of a person in whose interest is founding and activity of the legal person or similar legal subject of a foreign law.

When performing the transaction based on the established business relationship amounting to EUR 15,000 or more, the bank is obliged to confirm the identity of the natural person who performs the transaction on behalf of the legal person, for example to establish and confirm the identity of the legal representative or authorised person directly inspecting their private documents, during their presence. If the transaction is performed by an authorised person, that person has to submit a verified written authorisation issued by the legal representative. The bank shall file the written authorisation issued by the legal representative or a client's authorised person.

If both the legal representative and authorised person are absent during the transaction (for example transactions through e-banking), the procedures that the bank requests during the use of a qualified digital certificate and a password to confirm the identity of the legal representative or authorised person during the process of transaction shall be applied.

3.1.3 Establishing the beneficiary owner of the legal person

As a part of establishing and confirming a client who is a legal person, the bank is obliged, besides the identification, to confirm the beneficiary owner of that legal person. With the purpose of gathering information, the bank shall implement the measures and operations to a person which is the beneficiary owner.

When it comes to the high-risk client, the bank must confirm the given data, if they were not received from the reliable and independent source (for example if the only source of data during establishing the identity of a client was a written statement of the legal representative, in that case the bank has to verify the data to the extent when it gains understanding about the ownership of the legal person and its control structure, in order to identify all beneficiary owners of the client.

The beneficiary owner of a company, i.e. a legal person in a sense of Article 19 of the Law is: (1) a natural person who, directly or indirectly, is the owner of more than 25% of the business share, the right to vote or other rights, based on which that person participates in management i.e. capital with more than 25% of share or has a prevailing influence in asset management of that company and

(2) a natural person who indirectly provides or is providing assets to the company and based on that has the right to significantly influence the decision making of the management bodies of the company during decision making on the financing and business.
According to the abovementioned definition, the beneficiary owner is a natural person which participates (directly or indirectly) in the management of a legal person, based on more than 25% of ownership share. During identification of the beneficiary owner, it is necessary to check the ownership share of a certain natural person in a legal person, as well as the ownership share of the legal person which is under control of that natural person.
The bank may receive information on ownership based on the original or a certified copy from the court register or other official register submitted by the legal representative or authorised person on behalf of the legal person. In addition, the bank may apply provisions of the Law which enable that the data regarding the beneficiary owner can be verified directly in the court register or other public register, or through other available sources. If all the required data referring to the beneficiary owner (for example the date and place of birth) cannot be obtained from a court register or other official register, the bank may obtain the missing data from the legal representative or its authorised person. A foreign owner is considered to be a company, legal person, as well as institution or other person of a foreign law, which is directly or indirectly the owner of at least EUR 500,000 of the business share of the stocks, i.e. share in the capital. The beneficiary owner of the institution or another person of a foreign law (trust, fund or similar) who accepts, manages or shares property assets for certain purpose, with the meaning of this Law is considered to be:
(1) a natural person who, directly or indirectly, disposes with more than 25% of the property of the legal person or a similar subject of foreign law, (2) a natural person who is appointed or definable as the owner of more than 25% of income from the managed assets.
The bank has to verify the structure of the ownership for the clients – legal persons and gather all necessary data related to the beneficiary owner, in accordance with the Law.
If the legal person has the registered office in Montenegro, the bank is recommended to perform direct verification in the court register or other public register, in order to gather or confirm data referring to the beneficiary owner of that legal person.
If one of beneficiary owners is a foreign legal person, the bank is recommended to gather data related to the beneficiary owner of that legal person based on the original or a certified copy from the foreign register (that cannot be older than three months) or from the business documents submitted by the legal representative or the authorised person on behalf of the client. Since the bank has no information regarding the validity of documents from another country, it is recommended that the legal representative of the client or authorised person deliver an electronic statement from the public register from another country.
If, due to objective reasons, the legal representative is unable to present required documentations which clearly show the data related to the owner, those data shall be provided from the written statement delivered by the legal representative or its authorised person. In addition, the bank will also request a written statement from the legal representative in case of doubt in validity of submitted data.
If the legal representative shows unwillingness to cooperate with the bank in providing necessary data and for that reason the beneficiary ownership cannot be determined, the bank should not establish a business relationship. If the business relationship is established, in situation when a client avoids submitting all data required by the law, it is advised to the bank to use it as the indicator for revealing a suspicious activity of a client related to money laundering and terrorism financing.
If the bank, in addition to undertaken measures, is unable to receive data related to the beneficiary owner (besides the detailed analysis of the ownership structure), due to the complexity of the structure itself, in such cases the bank is allowed to establish (or continue) such business relationship, providing that the bank gathers written statement of the legal representatives or the

authorised person and classifies such client as a high-risk client, which needs enhanced due diligence of business activities. It should be mentioned that this is applied in exceptional cases, and is not usual practice. In the case of following the procedure of establishing a legal person's beneficiary owner referred to above, the bank is obliged to prove to the authorised supervisory body that it has implemented in appropriate manner the procedure to establish the beneficiary owner, and it is the complex ownership case which justifies the bank's conduct. At the same time, the bank is advised to evaluate the complex ownership structure as a possible reason to report suspicious transactions.
Besides, banks should request from their clients written information on each change of beneficiary owners. The internal acts of banks should define the procedure for determining the beneficiary owner, taking into account the provisions of the Law referred to above.

3.2 The manner of establishing the client's acceptability

By the means of the internal act, the bank is obliged to determine the conditions for the assessing the acceptability of a client on the basis of gathered and verified data and information on the client before establishing the business relation. This is the procedure that includes the identification of a client and the beneficiary owner, and if the client is a legal person, gathering information on the purpose and the nature of the business relation or transaction and other information with the meaning of Article 11 paragraph 1 of the Law. Beside the abovementioned procedure, Article 11 paragraph 2 of the Law prescribes that a bank may exceptionally perform stipulated due diligence measures during the establishment of the business relation with the client, if it is necessary for the purpose of establishing the business relation and if there is insignificant risk of money laundering or terrorism financing.
When it identifies, i.e. gathers and verifies all data on a client stipulated by the Law, the bank establishes the business relation with the client.
By the means of the internal act, the bank shall also define reasons to reject entering into business relationship with the client, and especially if: the state of origin of the client or the client's beneficiary owner is on the list of non- cooperative countries, issued by the Financial Action Task Force (FATF), on the list of countries stated as "off-shore" zones or the list of countries considered by the supervisory body as countries exposed to risk;
the client or client's beneficiary owner is a person from the country against which measures of the UN Security Council Resolutions have been undertaken;
the client is a person form the List composed according to the UN Security Council Resolutions.

3.3. Risk assessment of individual client, group of clients and business relationship
The bank performs the risk assessment of an individual client or a group of clients on the basis of risk analysis approach. Before the creation of a client's risk assessment, the bank is obliged, in addition to the identification, the bank is obliged to conduct client due diligence the identification, within the meaning of Article 9 of the Law, and especially in the following **cases**: (1) when entering into business relationship with a client, (2) in the case of one or more related transactions amounting to EUR 15 000 or more, (3) when there is doubt into the accuracy and the authenticity of gathered data on a client's identification, (4) when there is a suspicion of money laundering or terrorism financing regarding a client or a transaction.
As a rule, the bank performs customer due diligence before establishing the business relationship or before performing the transaction and only exceptionally when establishing business relation, if there is insignificant risk of money laundering or terrorism financing. In the case when the bank has established the business relation to the client and the client performs one or more related transactions amounting to EUR 15 000 or more, the bank shall collect only additional data (e.g. the purpose of transaction, data on source of assets, data on receiver of assets, and the like). **The**

measures the bank is obliged to perform in the customer due diligence procedure include:

- identification of a client or the beneficiary owner, if a client is a legal person;
- gathering and verification of data on client, i.e. the beneficiary owner, or if a client is a legal person gathering data on the purpose and the nature of the business relationship or transaction and
- after establishing the business relation, the bank shall regularly monitor business activities of the client and it shall verify the compliance of these activities with the nature of business relationship and the usual scope and the type of client' operations.

The table below shows the cases in which the bank is obliged to perform standard client due diligence, as well as the measures to be overtaken in order to perform client due diligence: Since the bank may neither perform business relationship nor perform transactions if all measures prescribed within the standard client due diligence have not been performed, a client's business activities shall continue to be monitored as long as the business relationship lasts.

Cases in which the bank is obliged to perform standard client due diligence					
		(1) when establishing business relation	(2) when performing one or more connected transactions amounting to EUR 15.000 and above	(3) when there is doubt into the accuracy and the authenticity of gathered data on a client's identification	(4) when there is a suspicion of money laundering or terrorism financing regarding a client or a transaction
Measures to be overtaken by the bank in order to perform client due diligence	(a) identification of a client	Yes	Yes	Yes	Yes
	(b) determining beneficiary owner	Yes	-	Yes (additional data)	Yes (additional data)
	(c) collecting required data	Yes	Yes	Yes	Yes
	(d) identification of a client when accessing the safe	Yes	-	Yes	Yes (when there is a suspicion of ML and TF regarding a client)
	(e) collection of additional data for the client which is a PEP	Yes	Yes	Yes	Yes

Besides the standard client due diligence, the bank shall dispose with special forms of client verification prescribed by the Law, including the: enhanced client verification and simplified client verification (described in Chapter 3.3.1).

After performing the verification of the client, the bank shall, on the basis of the risk factors, classify the client into a certain category of money laundering and terrorism financing risk. Taking into account the fact that the risk analysis of money laundering and terrorism financing requires proper information on the client and its operations, it is recommended that the classification of the client by risk categories is performed by the organisational unit which knows

the client the best together with the compliance officer for the purpose of detecting and prevention of money laundering and terrorism financing.
Immediately after establishing business relationship, the bank shall determine the so-called initial risk profile of a client and it shall classify the client into the appropriate risk category. Besides the classification of new clients and determining their risk profiles, the bank is obliged to also classify the existing clients.
During the duration of the business relationship with the client and monitoring its business activities, the bank is obliged to update all data and to classify the client into the appropriate category. This means, for example, if a bank determines that the some client's operations are significantly distracting his regular operations, the bank has to perform additional analysis of a client's operations, in order to determine the reasons for such distracting. On the basis of the additional analysis, compliance officer has to estimate the client's risk profile and if necessary, to reclassify it. Banks are also recommended to establish procedures for regular update regarding the assessment of the risk profile of a client to which there are no significant violations of the normal operations. This may be done during the regular updating of documents and the data on the client.
By the means of the internal act, the bank shall determine the dynamics of risk assessment of clients depending on the client itself and its operations.
If a client, on the basis of risk factors, may be classified into different risk categories referring to money laundering and terrorism financing, the client shall be assigned only one risk profile presenting the highest risk.

3.3.1 Special types of client verification

The Article 24 of the Law stipulates the following special types of client verification:

- Enhanced client verification and
- Simplified client verification.

The bank is obliged, along with identification of a client, to undertake additional measures for client verification during:

- concluding an open account relationship with a bank or other similar credit institution, with a headquarters outside the EU or outside the countries from the List;
- concluding a business relationship or performing transactions from Article 9 paragraph 1 item 2 of this Law with a client, who is a politically exposed person as defined in Article 29 of this Law;
- verification of a client who is not present during identification and verification of the identity.

The bank is obliged to apply the measure or measures of enhanced client verification referred to in Article 26 (open account banking relationship with a credit organisations of a third country), Article 27 (politically exposed persons) and Article 28 (identifying a client in absence) of the Law, in the cases when it estimates that, due to the nature of the business relationship, form and manner of performing business transactions, business profile of a client, or other circumstances related to the client, there is or may occur a risk of money laundering or terrorism financing.

3.3.1.1 Enhanced client verification

a) Open accounts and banking relationships with banks from third countries

Relationship of an open account relation is a contract relationship between domestic and foreign credit organisation, created by opening a bank account of a foreign credit organisation with the domestic credit organisation (for example, opening of loro account). Article 26 of the Law

prescribes that open account relationship with a bank with headquarters in third country presents an increased risk and therefore requires that bank performs additional verification and due diligence of the client, which is illustrated in table below:

Open account relationship with a bank with headquarters in a third country				
Case stipulated by the law ↓	1) Authorisation of compliance officer in the bank ↓	2) Receiving additional documentation and data ↓	3) Additional verification and client due diligence of business ↓	4) Additional measures ↓
Open account relationship with banks from third countries	Yes	Yes (data defined by Article 26 of the Law)	Yes	Upon bank's assessment

Bank employees in charge of concluding contracts on open accounts relationships with the bank or similar financial organisation with headquarters in a country outside of EU or a country not listed at the list of countries who do not comply with standards in area of prevention of money laundering and terrorism financing, are obliged, before concluding the contract, to undertake the procedure of enhanced verification of the client and to provide written agreement of the complying officer in the bank.
The bank gathers the required data from public or other available records, i.e. by verifying the personal and business documents, delivered by the bank or other similar credit organisation with the registered office outside of EU and outside countries on the list. Data the bank is required to provide in the case of concluding an open account relationship with a bank from a country outside of EU or outside countries from the list include:

- date of issuance and duration of validity of licence for performing banking services, title and the registered office of the relevant state body that issued the licence;
- description of implemented internal procedures, related to exposure and prevention of money laundering and terrorism financing, and especially procedures of client verification, verification of the real owners, reporting data on suspicions transactions and clients to the relevant bodies, record keeping, internal control and other measures which the bank, or other similar credit organisation, performed with regards to prevention and revealing of money laundering and terrorism financing;
- description of a system setting in area of revealing and prevention of money laundering and terrorism financing, applied in third country, where the bank or other similar credit organisation has headquarters and is registered;
- written statement that the bank or other similar credit organisation in country where it has headquarters, i.e. where it is registered is under legal supervision and that, in accordance with the laws of that country, it is obliged to apply adequate regulations in the area of revealing and prevention of money laundering and terrorism financing;
- written statement that the bank, or another similar credit organisation, is not doing business as a "shell-bank";
- written statement that the bank or another similar credit organisation has no established relations and is not establishing business relationships and does not perform transactions with "shell-banks".

In the cases that the bank has concluded an open account relationship with a bank outside the EU or outside of the List of countries, before the Law came into force, the bank is obliged to request and gather all required data and information regarding the bank. If the bank does not receive all the requested data, it is recommended that the bank should discontinue such open account banking relationship.

b) Client as politically exposed person

1. The procedure to include persons on the list of politically exposed persons
Pursuant to Article 27 of the Law, a politically exposed person is a natural person which acts or has acted during previous year on a high public position in the state, including members of immediate family and close associates.
In order to determine politically exposed persons and members of immediate family and close associates with the meaning of the Law, the bank can act in one of the following ways:

- the client fills out the form (enclosed to these guidelines and representing its integral part, the form PEP);
- gathering information from public sources;
- gathering information based on accessing database including lists of politically exposed persons (World Check PEP List, inquiry through internet, etc.).

The procedure of establishing close associates of politically exposed persons is applied if the bank estimates that, based on documented facts, such relationship exists.
The bank is obliged to identify clients pursuant to the Law, and at the same time, in one of the manners described in paragraph **2** of this section, to determine whether a client is the politically exposed person. Upon determining that the client is a politically exposed person, a bank employee is obliged to perform enhanced client verification (Article 25 of the Law) which includes additional measures in the cases of:

- concluding business relationship or performing transactions referred to in Article 9 paragraph 1 item 2 (performing one or more transactions amounting to EUR 15,000 or more);
- assessing that, due to nature of the business relationship and manner of performing the transaction, the business profile of a client, i.e. other circumstances related to the client, there is or there might be a risk of money laundering or terrorism financing.

In addition, as a part of enhanced client verification – politically exposed person, pursuant to the Law, a bank employee is obliged to: provide written consent of complying officer from the bank, before establishing business relationship with a client.

- provide data on source of property and assets which are the subject of a business relationship, i.e. transaction, from personal and other documents submitted by the client, and if it is not possible to acquire needed data from submitted documents, the data are provided directly from client's written statement;
- carefully follow transactions and other business activities performed at the bank by politically exposed person after establishing business relationship, especially bearing in mind the purpose and intention of transaction as well as the compliance with its usual business.

Additional measures implemented in procedure of a client extended verification

Case prescribed by law ↓	1) Authorisation of the compliance officer in the bank ↓	2) Receiving additional documentation and data ↓	3) Additional verification and client due diligence of business ↓	4) Additional measures ↓
Politically exposed person	Yes	Data defined by Article 26 of the Law	Yes	Upon bank's assessment

The bank is obliged to establish a list of politically exposed persons, which will in an adequate manner be available to bank employees with direct contact with clients.

2. Procedure of cessation of obligation to treat a person as politically exposed person.
The bank is obliged to establish the procedure of cessation of treating a client as politically exposed person with an internal act. That implies bank's obligation that after one year of cessation of acting as a politically exposed person on a prominent position within a county, that person, as well as members of their immediate family and associates, should be excluded from the list of politically exposed person. After establishing a business relationship with a politically exposed person, members of their immediate family and associates in accordance with the Law, the bank is obliged to keep special records about such persons and transactions.
The bank is obliged to update their list of politically exposed persons on regular basses, in order to implement the procedure of extended verification of a client pursuant to the Law and for those clients who at the time of starting a business relationship were not publically exposed persons with the meaning of the Law.

c) Establishing client's identity in absence
With the meaning of Article 28 of the Law regarding identifying and verification of client's identity in absence, the bank is obliged within enhanced client verification, along with identification referred to in Article 7, to undertake one or more additional measures, such as:

- provide additional documents, data or information, based on which the client's identity is verified;
- verify provided documents or provide a certificate from a foreign financial organisation which performs payment services that the first payment of the client was made on the debt of the account held by that organisation. Additional documents, data or information based on which the clients' identification is verified may be as follows:
- for residents a prove on residence issued by the relevant state body which keeps record on residence;
- personal references (for example if it is possible to receive references from another bank's client);
- previous references from the bank related to the client;
- data on source of assets and property which are or will be the subject of a business
- relationship;
- certificate on employment of a public function performed by the client.

For natural persons, banks may additionally verify submitted documents in at least one of the following ways:

- confirming the date of birth by using official personal document (for example birth certificate, passport, or other public records);
- confirming the permanent address (for example by using an TFN, bank statement, or a letter issued by a public institution);
- contacting a client by phone, letter or electronic mail in order to confirm gathered information after the bank account was open (for example, non-operating phone line, returned letter of incorrect e-mail address should indicate that additional verification is needed).

For legal persons, banks may additionally verify submitted documents in at least one of the following ways:

- reviewing financial reports and other documents about business;
- reviewing public registers or other inquiries in order to establish that legal person
- is still in business, that is was not deleted from the register or is not in bankruptcy, or that it is not in process of ceasing the business, being deleted from the register or bankruptcy;
- independent verification of information, such as using public and private databases;
- contacting client via phone, mail or electronic mail.

3.3.1.2 Simplified verification of a client

As a part of a special verification of a client, a bank may during establishing business relationship or during performance of one or several connected transfers amounting to EUR 15,000 or more, apply simplified verification of clients with residence in EU or is on the list of countries issued by the Ministry of Finance of Montenegro.

With the meaning of Article 29 of the Law, low risk clients to whom the simplified client verification is implemented include:

- branch banks of foreign banks and other financial organisations, savings banks and savings-loan organisations, post offices, associations for management of investment funds and branch offices of foreign associations for management of investment funds, associations for management of retirement funds and branch offices of foreign associations for management of retirement funds, life insurance companies and branch offices of foreign life insurance companies which perform life insurance services, organisers of classic and special lottery games
- state body or body of local government and other legal persons performing public authority; company whose securities are included in trade on organised market in countries which are EU members or other countries which apply EU standards;
- clients referred to in Article 8 paragraph 4 of this Law, for which there is insignificant risk of money laundering and terrorism financing.

In case when the client has a insignificant risk of money laundering and terrorism financing, the bank shall, during simplified client verification, implement fewer measures for client due diligence. In accordance with that, bank is not obliged to verify the client, nor is it necessary to

establish the beneficiary owner. The data the bank is obliged to gather in the procedure of simplified client verification are given in table below:

Simplified verification and client due diligence – data on client being a legal person	
Client data	□ company, □ legal person's registered office, i.e. on whose behalf and for whose account the business relationship is established.
Data on establishing business relationship	□date of establishing business relationship □purpose and nature of establishing business relationship
Data on performed transactions pursuant to Article 9 paragraph 1 item 2 of the Law, i.e. on one or more connected transactions amounting to EUR 15,000 or more	□company and registered office of the legal person, on whose behalf and for whose account the transaction is made; □name of the representative or authorised person who on behalf of the legal person performs transaction; □date and time of transaction; □amount of transaction, currency and manner of transaction; □purpose of transaction and name and residence, i.e. company and residence of legal person for whom the transaction is intended for. We note that the bank gathers the abovementioned information by inspecting the original or certified copies of documents issued by the CRCC, delivered by the client, or by direct inquiry. If the listed data cannot be obtained, the missing data are taken from the original or certified copies of personal documents and other business documentation, submitted by the client or written statement of the representative or authorised person. Date of issuance of the documents must not be older than three months.
Data on a person representing the client (legal representative or authorised person).	Proscribed data for legal representative or authorised person, requested for those persons during regular verification of the client.

It should be noted that the performing of simplified client verification is allowed only for clients (legal persons) defined by Article 29 of the Law and who comply to its provisions,
i.e. do not perform suspicious transactions, as well as that the bank cannot enlarge the number of clients to which the simplified client verification would be performed. Besides the above mentioned legal requirements that the bank is obliged to perform during the simplified client verification procedure, the bank is recommended to:

- identify unusual and suspicious activities;
- deliver data and documents upon the request of authorised state body and
- implement certain measures regarding the specific case. With its regards, it is recommended to the bank to also provide regular due diligence of business activities of those clients. It is also recommended in such cases that the bank should create a risk profile of a client and follow activities on regular bases in accordance with the established risk profile of that client. Frequency and scope of bank's activities should be adjusted with the low level risk, bearing in mind client's category.

3.3.2 Risk factors determining the risk level of a client or group of clients and business relationship

Internationally accepted standards that serve as a basis of methodology for risk-based approach for prevention of money laundering and terrorism financing (e.g. FATF and Wolfsberg guidelines), include the following risk factors:

Client risk factor: risk factors related to client's status or activities (for example state body, politically exposed person, client whose activities are related to cash transactions, non profit organisations, and the like)

Risk factors related to business relationship: risk of business relationship, e.g. with a client whose country of origin does not follow standards in the prevention of money laundering and terrorism financing, politically exposed person and other business relationships which according to bank's estimation are of high risk.
Risk factors related to geographic region: countries with inadequate systems for prevention of money laundering and terrorism financing, countries with high level of corruption or criminal activities, countries against which were announced restrictive measures by international organisations;

Risk factors determining risk level of a certain client or groups of clients, business relationship and well as risk factors related to geographical region are illustrated in the following risk matrix. Albeit the factors presented in matrix, the bank may define additional factors related to specific nature of client's business activity.

	Client risk factor
K1	**Insignificant risk** The client to which the bank performs simplified verification in accordance with the Law, i.e. the client with headquarters in EU or belongs to the countries from the list established by the Ministry of Finance of Montenegro, is evaluated as a client with insignificant risk: branch offices of foreign banks and other financial organisations, savings banks and savings-loan organisations, post offices, associations for management of investment funds and branch offices of foreign associations for management of investment funds, associations for management of retirement funds and branch offices of foreign associations for management of retirement funds, life insurance companies and branch offices of foreign life insurance companies which perform life insurance services, organisers of classic and special lottery games (obligors from Article 4 paragraph 2 items 1, 2, 3, 4, 5, 6, 8 and 9); state body or a local government body and other legal persons performing public authority; company which securities are included in trade on organised market in countries which are EU members or other countries which apply EU standards; clients referred to in Article 8 paragraph 4 of the Law, for which there is slight risk for money laundering and terrorism financing.

K2	**Low level risk** The client is classified into this category based on verification directly after establishing business relationship and which satisfies all legally stipulated requests, a client to which the bank during due diligence procedure has not noticed violation of usual business activities, and to which the bank does not apply neither nor simplified verification in accordance with the Law.
K3	**Middle level risk** The client is classified into this category based on verification, due diligence and evaluation that the customer cannot be placed in category with insignificant risk, low risk or high risk level, and the bank has notices some deviations in regular business activities while performing due diligence.
K4	**High risk** The bank performs extended verification in accordance with the Law towards that client, and a client where while performing due diligence of business activities the bank has noticed significant discrepancy from usual business activities, and especially: the client cannot prove the source of assets, or the source of assets is unknown or unclear; the client was not present during identification and verification of identity; there is a suspicion that the client acts upon instructions or order of a third person; there is unusual route of transaction, especially regarding the purpose, amount, mode of performance, purpose and similar; there are indications that client performs suspicious transactions; client is politically exposed person with the meaning of Article 2 of the Law, and bank performs extended verification referred to in Article 25 paragraph 1 item 2; the bank account of the client is connected with accounts of clients with higher risk; the client whose legal representative, authorised person or the real owner is a politically exposed person; the client is a foreign legal person who is forbidden to perform certain activities (for example trade, manufacturing or other activity) in country where it is registered or foreign legal person registered in a country where registration of off-shore companies is allowed; the client with complex legal layout or ownership structure where it is difficult to establish the real owner; client is a financial organisation which does not request or is not obliged to receive authorisation from the relevant body to perform business activity or is not obliged to implement measures related to prevention of money laundering and terrorism financing in accordance with the legislation of the country of origin; client that bank has delivered reports on suspicions transaction to the relevant supervisory body within the last three years; the client for which the relevant supervisory body gave order about temporary cancelation of transaction or request for permanent due diligence; the client is a person listed on internal black list of the bank or the banking group.
	High risk factors in business relationship
BR	Business relationship with a client to which the bank implements enhanced verification measures pursuant to the Law include: business relationship with a bank from the third country; business relationship with politically exposed person.
	High risk factors related with geographic region

G1 **G2** **G3** **G4**	High risk countries where client has residence i.e. permanent residence (natural persons) or headquarters for legal persons, includes the following countries : □countries with enforced sanctions, embargo or similar measures by United Nations; □countries for which the relevant international bodies or organisations have established a) the lack of adequate laws, regulations and other measures to prevent money laundering and terrorism financing; b) financing or supporting terrorism activities or that terrorist organisations are active in those countries; c) the significant level of corruption or other criminal activities; □countries which are not members of European Union or signatories of the Agreement on the European Economic Area nor they belong to the equivalent third countries; □which, according to the international organisation FATF, belong to a non-cooperative countries or territories and in case of off-shore financial centre listed on the document prepared by the relevant body.

3.4 Risk factors related to products/transactions relate to: sensibility of the product or service regarding their misuse for purpose of money laundering or terrorism financing (for example electronic money transfer).

	Risk factors related to products or transactions of high risk
	Risk factors related to products or services of high risk are related to sensibility of the product or service regrinding their misuse for purpose of money laundering or terrorism financing, such as:
P/T 1 **P/T 2** **P/T 3**	□international services of correspondent banks of third countries which include commercial payments; □for persons who are not clients of the bank (for example if a person is using the service of a bank which acts as intermediary bank; □services which insure higher level of anonymity, such as electronic banking, international money transfer or similar. . □cash transactions ; □occasional transactions which are not consistent with client's activities or with expected purpose of an account. .

3.5 Risk categories of clients

Classification of a client and groups of clients into certain risk category based on defined risk factors		
Category of risk	**Code of risk**	**Risk factor**
Insignificant risk	A	The bank classifies a client in category A if the bank applies simplified verification pursuant to the Law (K 1).
Low level risk	B	The bank classifies a client in category B, immediately after establishing a business relationship (to which a simplified verification pursuant to the Law is not applied, i.e. the client is not classified into category A) and a client to which while performing due diligence client's business activities the bank did not notice discrepancy from regular business activities (K2).

Middle level risk	C	The bank classifies a client in category C, where during due diligence the bank has noticed some discrepancies from regular business activities. (K3).
High level risk	D	The bank classifies a client in category D (K 4) : the bank has noticed significant discrepancy from regular business activities; to whom high risk factors are related with the geographic region (G1, G2, G3, G4); client is related with high level risk factors regarding business relationships (BR); client is related to high level risk factors regarding the product or service (P/T 1, P/T2 and P/T 3).

Note: With regards to the information on risk countries i.e. non-cooperative countries or territories which do not fulfil the key international standards related to money laundering or terrorism financing please refer to internet pages of relevant international bodies:
MONEYVAL: www.coe.int/t/dghl/monitoring/moneyval and
FATF: www.fatf-gafi.org

3.6 Monitoring client's accounts and transactions

A bank is obliged to continuously perform appropriate measures to detect unusual or suspicious activities based on the list of indicators for the identification of clients and transactions which reasonable grounds to suspect money laundering or terrorism financing. All clients must be included in this procedure, regardless of their risk profile.
A bank also has to establish appropriate procedures for due diligence of client's business activities, whereas the scope and implemented measures have to be consistent with the client's risk profile. The measures to be implemented by the bank to the client classified into appropriate risk category are given in the table below:

Measures to be taken by a bank with a view to monitoring clients classified into risk categories			
Risk category	**Code of risk category**	**Customer due diligence**	**Monitoring**
Insignificant risk	A	Simplified client due diligence	Annual
Low risk	B	Standard client due diligence	Semi-annual
Middle risk	C	Standard client due diligence, with additional necessary measures as assessed by the bank	Quarterly
High risk	D	Enhanced customer due diligence	Monthly

3.7 Risk management that the bank is exposed to in area of prevention of money laundering and terrorism financing

The bank is, pursuant to the Law, obliged to manage all risks it is exposed to in its activities, which includes risk management regarding money laundering and terrorism financing.
In this sense, the bank is obliged to establish a system for managing risk from money laundering

and terrorism financing, which shall provide:
identification of risks coming from the existing risks or those that may originate from

- new business products or bank activities;
- risk measurement by setting up mechanisms and procedures for accurate and due risk
- assessment;
- due diligence and risk analysis;
- control and minimising the risk.

The risk management system has to be appropriate to the size of the bank, complexity ofoffered products and services in its business activities. The risk management system regarding money laundering and terrorism financing shall include at least:

- developed processes for risk management;
- clearly defined authorisation and responsibilities for risk management;
- efficient and reliable system of information technology;
- manner and dynamics of reporting and informing the Board of Directors and bank management on risk management.

For the purpose of adequate risk management in area of prevention of money laundering and terrorism financing, the bank is obliged to decrease exposure to risk which is outcome of new technologies which enable anonymity (electronic or internet banking, electronic money, etc.), and in that sense the policies and procedures issued by the bank shall especially define:
identification of a customer using electronic banking;

- validity of signed electronic document;
- reliable measures against forging documents and signatures on documents;
- systems which ensure and enable safe electronic banking;
- other conditions in accordance with positive regulations which regulate the above mentioned area of business activities.

Banks must have policies and procedures that shall require complete information on the purpose and the nature of the business relationship or regarding the transaction with absent clients and they are obliged to apply them while establishing the business relationship with the client or when performing the enhanced client verification.

For the purpose of secure identification of a client using electronic banking, the bank may use various methods of identifications, including PINs, passwords, smart cards, biometrics and qualified electronic certificates.

3.7.1. Measures for prevention of terrorism financing based on risk-based approach

Unlike money laundering, terrorism financing has different characteristics and therefore risk based approach regarding terrorism financing requires more complex set of factors for risk assessment as well as more complex methods in order to establish the existence of terrorism financing.
The nature of source of terrorism financing can be different depending on terrorist organisations, bearing in mind that assets used for financing terrorist activities can result from both legal and illegal sources. When the sources of financing terrorist activities are resulting from criminal activities, the approach based on risk assessment of money laundering is applicable to terrorism financing as well. Bearing in mind that the transactions referring to terrorism financing are usually implemented in small amounts, those transactions, regarding their amount through application of risk-based approach on money laundering, are considered as low risk transactions, and therefore it is complicated to identify terrorism financing.

In the cases when sources of financing terrorist activities result from legal sources, it is even more difficult to identify that legally acquired assets are used for terrorist purposes. With its regards, some activities for preparation of terrorist activities can be unhidden, such as the procurement of necessary material or payment of certain services.
The problems of identifying terrorism financing are complex, therefore various institutions and state bodies are dealing with the problem, while the obligation of the bank particularly regarding the reporting to the Administration for Prevention of Money Laundering and Terrorism Financing about suspicious transactions which could be related to terrorism financing. With its regards, it is very important that the banks supervise cash transactions and transactions with countries for which relevant international organisations or bodies have determined to finance or assist terrorist activities.

3.8 Professional training and improvement of bank employees

The important element of the efficient system for prevention of money laundering and terrorism financing is adequate and timely training and development of professional skills of employees performing tasks of identifying and preventing money laundering and terrorism financing. Professional training of employees referring to prevention of money laundering and terrorism financing measures must include good knowledge of regulatory requests and internal politics and procedures adopted by the bank in order to successfully manage risks in this area.
All employees, whose tasks are anyhow related to the implementation of measures related to prevention of money laundering and terrorism financing, have to be included in the professional training program.
Training needs have to be adjusted to the special needs of employees according to individual lines of work, i.e. according to the specific tasks they perform. In that sense, the techniques in identifying and prevention of money laundering has to be presented to employees working as bank tellers and to employees working in other sectors involved in the programme of identifying and prevention of money laundering and terrorism financing.
Special attention should be paid on newly hired employees, who need to be informed about the basic measures undertaken in the bank regarding identification and prevention of money laundering and terrorism financing.
In addition, it is very important to educate compliance officers and their deputies in order to enable them to recognise new forms, techniques and trends related to money laundering and terrorism financing. It implies their information and update to legal and regulatory changes in order to adjust internal acts with new regulations timely.
The management of the bank has to be informed with the risk that the bank may face due to lack of compliance with regulations in the money laundering and terrorism financing area, as well as due to inadequate training of employees who are, as part of their duties, obliged to implement measures on the prevention of money laundering and terrorism financing.
The bank has to keep adequate records on completed education, especially with regards to persons included in education, date of seminars, courses, workshops, etc.
Professional training and improvement of bank employees related to prevention of money laundering and terrorism financing has a goal to raise awareness of the employees about the importance of timely undertaken measures for prevention of money laundering and terrorism financing.

1 Banks shall harmonise their internal acts to these Guidelines as well as perform other activities necessary for applying these Guidelines within 60 days of their publishing.
2 These Guidelines shall come into force on the day following their publishing at the website of the Central Bank of Montenegro.

THE COUNCIL OF THE CENTRAL BANK OF MONTENEGRO
No.:0101- 258/2-8 President of the Council
Podgorica, 25.02.2010 Ljubiša Krgović

FORM FOR IDENTIFICATION OF A POLITICALLY EXPOSED PERSON Form: PEP

With the meaning of Article 27 of the Law on Prevention of Money Laundering and Terrorism Financing (hereinafter: the Law), OGM 14/07 and 4/08), a bank shall determine whether the client is a politically exposed person. **FORM FOR IDENTIFICATION OF A POLITICALLY EXPOSED PERSON Politically exposed person**, with the meaning of the Law, is a natural person that is acting or has been acting in the last year on a distinguished public position in a state, including his/her immediate family members and close associates. **Members of a politically exposed person's immediate family** are a marital or extra-marital partner and children born in a marital or extra-marital relationship and their marital or extra-marital partners, parents, brothers and sisters. **A close associate of a politically exposed person** is a natural person that has a common profit from the asset or established business relationship or other type of close business contacts. Pursuant to the Law, please answer the following questions:

Table 1

Are you a natural person that is acting or has been acting in the last year on a distinguished public position in a state?

1.	president of a country, prime minister, minister, deputy or assistant minister, head of public administration body or local administration body or its deputy, other officials;	YES	NO
2.	elected member of Legislative body (members of parliament and all other persons appointed/elected by the parliament);	YES	NO
3.	carrier of the highest legal and constitutionally-court functions (judges, plaintiffs and their deputies);	YES	NO
4.	a member of the Audit courts, i.e. supreme Audit institutions and the Central Bank Councils;	YES	NO
5.	ambassador, consul or the general officer of the armed forces	YES	NO
6.	a member of management or supervisory body of an state owned enterprise	YES	NO

Table 2

Are you an immediate family member of a person referred to in table 1?

1.	marital or extra-marital partner;	YES	NO
2.	children born in a marital or extra-marital relationship and their marital or extra-marital partners;	YES	NO
3.	parents, brothers and sisters.	YES	NO

Table 3

Are you a close associate of a person referred to in table 1?		
1. do you have a common profit from the asset or established business relationship or other type of close business contacts;	YES	NO
2. are you in some other type of closer business contact with persons referred to in Table 1?	YES	NO

Table 4		
Data which client submits to a bank after the expiry of 12 months from the day when his acting at the public function expires, pursuant to which the bank is not longer obliged to treat the client as an politically exposed person.		
1. Did the 12 months period from the day when your public function in the State expired?	YES	NO
2. Are you a family member or a close associate of a physical person's that acted at the public function referred to point 1 of this table?	YES	NO
If your answer to any of the questions above in Tables 1, 2 or 3 was YES, you are, pursuant to the Law on Prevention of Money Laundering and Terrorism Financing classified as a Politically exposed person. Therefore, please state the origin of assets or property which are, or shall be the subject of business relation or transaction**:** **In hereby confirm that the abovementioned data are true.** Client's name and surname Client's address Client's date of birth Place and date Client's signature Name and surname of a bank's employee Place and date Signature of a bank's employee **I agree to establish business relations and/or perform transaction with a politically exposed person.** Name and surname of the responsible person in a bank Place and date Signature of the responsible person in a bank		