COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

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

MONEYVAL(2013)15ANN

Report on Fourth Assessment Visit – ANNEXES

Anti-Money Laundering and Combating the Financing of Terrorism

CROATIA

17 September 2013

Croatia is a member of MONEYVAL. This evaluation was conducted by MONEYVAL and the mutual evaluation report on the 4th assessment visit of Croatia was adopted at its 42nd Plenary (Strasbourg, 16-20 September 2013).

LIST OF ANNEXES

ANNEX I Details of all bodies met on the on-site mission - Ministries, other government authorities or bodies, private sector representatives and others

Ministries and other Government Authorities
Ministry of Finance (Anti-Money Laundering Office)
Ministry of Interior
Ministry of Justice
Ministry of Foreign and European Affairs
Ministry of Administration

Investigation and Law Enforcement Bodies and Public Prosecutor' Office
State Attorney's office
Office for Suppression of Corruption and Organised Crime
Security Intelligence Agency
Police National Office for Suppression of Corruption and Organised Crime

Financial Sector Bodies
Financial Inspectorate
Croatian National Bank
Croatian Financial Services Supervisory Agency

Other Government Bodies
Tax Administration
Customs Administration
Commercial Courts
Croatian Government's Office for Associations
State Audit Office
Judges from the Supreme Court of the Republic of Croatia
Government Agency for Managing State Owned Assets
Judges from the County Court in Zagreb

Private Sector Representatives and Associations
Croatian Bank Association
Croatian Post
Private Banks
Zagreb Stock Exchange
Croatian Chamber of Commerce
Notaries Public Chamber
Croatian Bar Association
Association of Accountants
Chamber of Auditors
Chamber of Tax Advisors
Real Estate Agents
Croatian Lottery
Representatives of organised game of chance

ANNEX II Designated categories of offences based on the FATF Methodology and Convention Offences

1. Designated categories of offence

Country		
	Criminal offenses in domestic law	
	The current Criminal Code Article no.	Criminal Law as of 1.1.2013. Article no.
Participation in an organised criminal group and racketeering;	333., 234.	328., 329., 243.
Terrorism, including terrorist financing	169.,187.a	97., 98.
Trafficking in human beings and migrant smuggling; Sexual exploitation, including sexual exploitation of children;	175.,177.	106.
Illicit trafficking in narcotic drugs and psychotropic substances;	173.	190.
Illicit arms trafficking	335.	331.
Illicit trafficking in stolen and other goods	236., 297.	244.
Corruption and bribery	294.a,, 294.b, 347., 348.	252.-254.,293.,294.,296.
Fraud	224.	236.
Counterfeiting currency	274.	274.
Counterfeiting and piracy of products	285.	261.
Environmental crime	250., 262.	193., 214.
Murder, grievous bodily injury	90.,91.,99.	110., 111., 118. -120.
Kidnapping, illegal restraint and hostage-taking	125.,124.	137., 136.
Robbery or theft;	216., 217., 218.	228. -230.
Smuggling	298.	256., 257.
Extortion	235.	243.
Forgery	311.	275. – 279.
Piracy	179., 180.	223.
Insider trading and market manipulation	Law on criminal offences against capital markets Art 3. and 4.	259., 260.

2. Conventions listed in the Annex of the FT Convention

Convention for the Suppression of Unlawful Seizure of Aircraft, done at The Hague on 16 December 1970	Ratified on **29 June 1972 (OG 33/1972)** **Article 223. para 1. of the Criminal Code**

Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation done at Montreal on 23 September 1971	Ratified on **29 June 1972 (OG 33/1972)** **Article 223. of the Criminal Code**
Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents, adopted by the General Assembly of the United Nations on 14 December 1973	Ratified on **10 December 1976 (OG54/1976)** **Articles 352., 353., 354. and 355. of the Criminal Code**
International Convention against the Taking of Hostages, adopted by the General Assembly of the United Nations on 17 December 1979	Ratified on **02 November 1984 (OG 9/1984)** **Articles 97., 137. and 353. of the Criminal Code**
Convention on the Physical Protection of Nuclear Material, adopted at Vienna on 3 March 1980	Ratified on **27 April 2001(OG 5/2001)** **Articles 97. and 219. of the Criminal Code**
Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, done at Montreal on 24 February 1988	Ratified on **27 October 1989 (OG 14/1989)** **Article 223. of the Criminal Code**
Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation, done at Rome on 10 March 1988	Ratified on **11 May 2005 (OG 4/2005)** **Articles 223. of the Criminal Code**
Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms located on the Continental Shelf, done at Rome on 10 March 1988	Ratified on **11 May 2005 (OG 4/2005)** **Article 223. of the Criminal Code**
International Convention for the Suppression of Terrorist Bombings, adopted by the General Assembly of the United Nations on 15 December 1997	Ratified on **20 April 2005 (OG 3/2005)** **Article 97. of the Criminal Code** **Article 215 of the Criminal Code** **Article 222 of the Criminal Code**

3. Implementation of the Vienna Convention

Provisions of the Vienna Convention	Croatian legislative acts and regulations that cover requirements of the Vienna Convention
Article 3 (Offences and Sanctions)	Art. 34, 37-38, 190-191, 244, 265, 303, 328-329 of the new Criminal Code
Article 4 (Jurisdiction)	Art. 10-18 of the new Criminal Code
Article 5 (Confiscation) - with regard to confiscation of proceeds derived from offences involving illicit trafficking of	Art 77-79 of the new Criminal Code

narcotic drugs or psychotropic substances; - with regard to seizure of property (assets); - with regard to rendering mutual legal assistance.	
Article 6 (Extradition)	Law on International Legal Assistance in Criminal Matters; Bilateral and multilateral agreements
Article 7 (Mutual Legal Assistance)	Law on International Legal Assistance in Criminal Matters; Bilateral and multilateral agreements
Article 8 (Transfer of Proceedings)	Law on International Legal Assistance in Criminal Matters; Bilateral and multilateral agreements
Article 9 (Other Forms of Cooperation and Training)	Bilateral and multilateral agreements
Article 10 (International Cooperation and Assistance for Transit States)	Bilateral and multilateral agreements
Article 11 (Controlled Delivery)	Article 332 of Criminal Procedure Code
Article 15 (Commercial Carriers)	
Article 17 (Illicit Traffic by Sea)	Criminal Procedure Code; Law on Police Activities and Powers
Article 19 (The Use of the Mails)	Article 332 of Criminal Procedure Code; Customs Service Act

4. Implementation of the Palermo Convention

Provisions of the Palermo Convention	Croatian legislative acts and regulations that cover requirements of the Palermo Convention
Article 5 (Criminalization of Participation in an Organized Criminal Group)	Art. 328-329 of the new Criminal Code
Article 6 (Criminalization of the Laundering of Proceeds of Crime)	Art. 37-38, 244, 265, 303 of the new Criminal Code
Article 7 (Measures to Combat Money-Laundering)	Anti-Money Laundering and Terrorist Financing Law
Article 10 (Liability of Legal Persons)	Law on the Liability of Legal Persons for Criminal Offences
Article 11 (Prosecution, Adjudication and Sanctions)	Criminal Code
Article 12 (Confiscation and Seizure)	Criminal Code; Criminal Procedure Code; Act on Proceedings for the Confiscation of Pecuniary Gain Resulting from Criminal Offences and Misdemeanours
Article 13 (International Cooperation for Purposes of Confiscation)	Criminal Procedure Code
Article 14 (Disposal of Confiscated Proceeds of Crime or Property)	Criminal Procedure Code; Act on Proceedings for the Confiscation of Pecuniary Gain Resulting from Criminal Offences and Misdemeanours
Article 15 (Jurisdiction)	Criminal Code
Article 16 (Extradition)	Law on International Legal Assistance in Criminal

	Matters
Article 18 (Mutual Legal Assistance)	Criminal Procedure Code; Law on International Legal Assistance in Criminal Matters
Article 19 (Joint Investigations)	Criminal Procedure Code
Article 20 (Special Investigative Techniques)	Article 332 Criminal Procedure Code
Article 24 (Protection of Witnesses)	Law on Protection of Witnesses
Article 25 (Assistance to and Protection of Victims)	Law on Police Activities and Powers
Article 26 (Measures to Enhance Cooperation with Law Enforcement Authorities)	Criminal Procedure Code
Article 27 (Law Enforcement Cooperation)	Criminal Procedure Code
Article 29 (Training and Technical Assistance)	Law on Police; Law on State Attorney's Office; Bilateral and multilateral agreements
Article 30 (Other Measures: Implementation of the Convention through Economic Development and Technical Assistance)	Direct application of Convention; Bilateral and multilateral agreements
Article 31 (Prevention)	Law on Police Activities and Powers; Law on State Attorney's Office
Article 34 (Implementation of the Convention)	Criminal Code

5. Implementation of the UN International Convention for the Suppression of the Financing of Terrorism

Provisions of the UN International Convention for the Suppression of the Financing of Terrorism	Croatian legislative acts and regulations that cover requirements of the UN International Convention for the Suppression of the Financing of Terrorism
Article 2	Art. 98 of the new Criminal Code
Article 3	Art. 10-18 of the new Criminal Code
Article 4	Art. 87 of the new Criminal Code
Article 5	Law on the Liability of Legal Persons for Criminal Offences
Article 6	Criminal Code
Article 7	Art. 10-18 of the new Criminal Code
Article 8	Art. 77-78 of the new Criminal Code
Article 9	Law on Police Activities and Powers; Criminal Procedure Code; Law on Foreigners
Article 10	Criminal Procedure Code; Law on International Legal Assistance in Criminal Matters; Bilateral and multilateral agreements
Article 11	Bilateral and multilateral agreements; Law on International Legal Assistance in Criminal Matters
Article 12	Bilateral and multilateral agreements; Law on International Legal Assistance in Criminal Matters; Criminal Procedure Code

Article 13	Bilateral and multilateral agreements; Law on International Legal Assistance in Criminal Matters; Criminal Procedure Code
Article 14	Bilateral and multilateral agreements; Law on International Legal Assistance in Criminal Matters; Criminal Code
Article 15	Bilateral and multilateral agreements; Law on International Legal Assistance in Criminal Matters; Criminal Code
Article 16	Bilateral and multilateral agreements; Law on International Legal Assistance in Criminal Matters; Criminal Procedure Code
Article 17	Law on Police Activities and Powers; Criminal Procedure Code; Croatian Constitution
Article 18	Criminal Code, AMLTF Law; Law on Police Activities and Powers; Criminal Procedure Code

6. Status of Implementation of the UN Security Council Resolutions

a) Resolution 1267 (1999)

Provisions of the Resolution 1267 (1999)	Croatian legislative acts and regulations that cover requirements of the Resolution 1267 (1999)
subparagraph "a" of paragraph 4	Law on International Restrictive Measures; Decision on the implementation of measures imposed by Resolutions 1267 (1999), 1333 (2000), 1363 (2001), 1373 (2001), 1390 (2002), 1452 (2002), 1455 (2003), 1526 (2004), 1617 (2005), 1735 (2006), 1822 (2008) and 1904 (2009) of the United Nations Security Council regarding sanctions against the members of the Alqaida organization, Usama bin Laden and the Taliban and other individuals, groups, undertakings and entities associated with them
subparagraph "b" of paragraph 4	Law on International Restrictive Measures; Decision on the implementation of measures imposed by Resolutions 1267 (1999), 1333 (2000), 1363 (2001), 1373 (2001), 1390 (2002), 1452 (2002), 1455 (2003), 1526 (2004), 1617 (2005), 1735 (2006), 1822 (2008) and 1904 (2009) of the United Nations Security Council regarding sanctions against the members of the Alqaida organization, Usama bin Laden and the Taliban and other individuals, groups, undertakings and entities associated with them

b) Resolution 1333 (2000)

Provisions of the Resolution 1333 (2000)	Croatian legislative acts and regulations that cover requirements of the Resolution 1333 (2000)
subparagraphs "a", "b", and "c" of paragraph 5	Law on International Restrictive Measures; Decision on the implementation of measures imposed by Resolutions 1267 (1999), 1333 (2000), 1363 (2001), 1373 (2001), 1390 (2002), 1452 (2002), 1455 (2003), 1526 (2004), 1617 (2005), 1735 (2006), 1822 (2008) and 1904 (2009) of the United Nations Security Council regarding sanctions against the

	members of the Alqaida organization, Usama bin Laden and the Taliban and other individuals, groups, undertakings and entities associated with them
subparagraphs "a", "b", and "c" of paragraph 7	Law on International Restrictive Measures; Decision on the implementation of measures imposed by Resolutions 1267 (1999), 1333 (2000), 1363 (2001), 1373 (2001), 1390 (2002), 1452 (2002), 1455 (2003), 1526 (2004), 1617 (2005), 1735 (2006), 1822 (2008) and 1904 (2009) of the United Nations Security Council regarding sanctions against the members of the Alqaida organization, Usama bin Laden and the Taliban and other individuals, groups, undertakings and entities associated with them
subparagraphs "a", "b" and "c" of paragraph 8	Law on International Restrictive Measures; Decision on the implementation of measures imposed by Resolutions 1267 (1999), 1333 (2000), 1363 (2001), 1373 (2001), 1390 (2002), 1452 (2002), 1455 (2003), 1526 (2004), 1617 (2005), 1735 (2006), 1822 (2008) and 1904 (2009) of the United Nations Security Council regarding sanctions against the members of the Alqaida organization, Usama bin Laden and the Taliban and other individuals, groups, undertakings and entities associated with them
subparagraphs "a" and "b" of paragraph 10	Law on International Restrictive Measures; Decision on the implementation of measures imposed by Resolutions 1267 (1999), 1333 (2000), 1363 (2001), 1373 (2001), 1390 (2002), 1452 (2002), 1455 (2003), 1526 (2004), 1617 (2005), 1735 (2006), 1822 (2008) and 1904 (2009) of the United Nations Security Council regarding sanctions against the members of the Alqaida organization, Usama bin Laden and the Taliban and other individuals, groups, undertakings and entities associated with them
subparagraphs "a" and "b" of paragraph 11	Law on International Restrictive Measures; Decision on the implementation of measures imposed by Resolutions 1267 (1999), 1333 (2000), 1363 (2001), 1373 (2001), 1390 (2002), 1452 (2002), 1455 (2003), 1526 (2004), 1617 (2005), 1735 (2006), 1822 (2008) and 1904 (2009) of the United Nations Security Council regarding sanctions against the members of the Alqaida organization, Usama bin Laden and the Taliban and other individuals, groups, undertakings and entities associated with them
subparagraphs "a" and "b" of paragraph 14	Law on International Restrictive Measures; Decision on the implementation of measures imposed by Resolutions 1267 (1999), 1333 (2000), 1363 (2001), 1373 (2001), 1390 (2002), 1452 (2002), 1455 (2003), 1526 (2004), 1617 (2005), 1735 (2006), 1822 (2008) and 1904 (2009) of the United Nations Security Council regarding sanctions against the members of the Alqaida organization, Usama bin Laden and the Taliban and other individuals, groups, undertakings and entities associated with them

c) <u>Resolution 1363 (2001)</u>

Provisions of the Resolution 1363 (2001)	Croatian legislative acts and regulations that cover requirements of the Resolution 1363 (2001)
paragraph 8	Law on International Restrictive Measures; Decision on the implementation of measures imposed by Resolutions 1267 (1999), 1333 (2000), 1363 (2001), 1373 (2001), 1390 (2002), 1452 (2002), 1455 (2003), 1526 (2004), 1617 (2005), 1735 (2006), 1822 (2008) and 1904 (2009) of the United Nations Security Council regarding sanctions against the members of the Alqaida organization, Usama bin Laden and the Taliban and other individuals, groups, undertakings and entities associated with them

d) Resolution 1373 (2001)

Provisions of the Resolution 1373 (2001)	Croatian legislative acts and regulations that cover requirements of the Resolution 1373 (2001)
subparagraphs "a", "b" and "c" of paragraph 1	Law on International Restrictive Measures; Decision on the implementation of measures imposed by Resolutions 1267 (1999), 1333 (2000), 1363 (2001), 1373 (2001), 1390 (2002), 1452 (2002), 1455 (2003), 1526 (2004), 1617 (2005), 1735 (2006), 1822 (2008) and 1904 (2009) of the United Nations Security Council regarding sanctions against the members of the Alqaida organization, Usama bin Laden and the Taliban and other individuals, groups, undertakings and entities associated with them
Paragraph 2	Law on International Restrictive Measures; Decision on the implementation of measures imposed by Resolutions 1267 (1999), 1333 (2000), 1363 (2001), 1373 (2001), 1390 (2002), 1452 (2002), 1455 (2003), 1526 (2004), 1617 (2005), 1735 (2006), 1822 (2008) and 1904 (2009) of the United Nations Security Council regarding sanctions against the members of the Alqaida organization, Usama bin Laden and the Taliban and other individuals, groups, undertakings and entities associated with them

e) Resolution 1390 (2002)

Provisions of the Resolution 1390 (2002)	Croatian legislative acts and regulations that cover requirements of the Resolution 1390 (2002)
subparagraphs "a", "b" and "c" of paragraph 2	Law on International Restrictive Measures; Decision on the implementation of measures imposed by Resolutions 1267 (1999), 1333 (2000), 1363 (2001), 1373 (2001), 1390 (2002), 1452 (2002), 1455 (2003), 1526 (2004), 1617 (2005), 1735 (2006), 1822 (2008) and 1904 (2009) of the United Nations Security Council regarding sanctions against the members of the Alqaida organization, Usama bin Laden and the Taliban and other individuals, groups, undertakings and entities associated with them

f) Resolution 1455 (2003)

Provisions of the Resolution 1455 (2003)	Croatian legislative acts and regulations that cover requirements of the Resolution 1455 (2003)
paragraph 1	Law on International Restrictive Measures; Decision on the implementation of measures imposed by Resolutions 1267 (1999), 1333 (2000), 1363 (2001), 1373 (2001), 1390 (2002), 1452 (2002), 1455 (2003), 1526 (2004), 1617 (2005), 1735 (2006), 1822 (2008) and 1904 (2009) of the United Nations Security Council regarding sanctions against the members of the Alqaida organization, Usama bin Laden and the Taliban and other individuals, groups, undertakings and entities associated with them
paragraph 5	Law on International Restrictive Measures; Decision on the implementation of measures imposed by Resolutions 1267 (1999), 1333 (2000), 1363 (2001), 1373 (2001), 1390 (2002), 1452 (2002), 1455 (2003), 1526 (2004), 1617 (2005), 1735 (2006), 1822 (2008) and 1904 (2009) of the United Nations Security Council regarding sanctions against the members of the Alqaida organization, Usama bin Laden and the Taliban and other individuals, groups, undertakings and entities associated with them
paragraph 6	Law on International Restrictive Measures; Decision on the implementation of measures imposed by Resolutions 1267 (1999), 1333 (2000), 1363 (2001), 1373 (2001), 1390 (2002), 1452 (2002), 1455 (2003), 1526 (2004), 1617 (2005), 1735 (2006), 1822 (2008) and 1904 (2009) of the United Nations Security Council regarding sanctions against the members of the Alqaida organization, Usama bin Laden and the Taliban and other individuals, groups, undertakings and entities associated with them

g) <u>Resolution 1526 (2004)</u>

Provisions of the Resolution 1526 (2004)	Croatian legislative acts and regulations that cover requirements of the Resolution 1526 (2004)
paragraph 4	Law on International Restrictive Measures; Decision on the implementation of measures imposed by Resolutions 1267 (1999), 1333 (2000), 1363 (2001), 1373 (2001), 1390 (2002), 1452 (2002), 1455 (2003), 1526 (2004), 1617 (2005), 1735 (2006), 1822 (2008) and 1904 (2009) of the United Nations Security Council regarding sanctions against the members of the Alqaida organization, Usama bin Laden and the Taliban and other individuals, groups, undertakings and entities associated with them
paragraph 5	Law on International Restrictive Measures; Decision on the implementation of measures imposed by Resolutions 1267 (1999), 1333 (2000), 1363 (2001), 1373 (2001), 1390 (2002), 1452 (2002), 1455 (2003), 1526 (2004), 1617 (2005), 1735 (2006), 1822 (2008) and 1904 (2009) of the United Nations Security Council regarding sanctions against the

	members of the Alqaida organization, Usama bin Laden and the Taliban and other individuals, groups, undertakings and entities associated with them
Paragraph 17	Law on International Restrictive Measures; Decision on the implementation of measures imposed by Resolutions 1267 (1999), 1333 (2000), 1363 (2001), 1373 (2001), 1390 (2002), 1452 (2002), 1455 (2003), 1526 (2004), 1617 (2005), 1735 (2006), 1822 (2008) and 1904 (2009) of the United Nations Security Council regarding sanctions against the members of the Alqaida organization, Usama bin Laden and the Taliban and other individuals, groups, undertakings and entities associated with them
paragraph 22	Law on International Restrictive Measures; Decision on the implementation of measures imposed by Resolutions 1267 (1999), 1333 (2000), 1363 (2001), 1373 (2001), 1390 (2002), 1452 (2002), 1455 (2003), 1526 (2004), 1617 (2005), 1735 (2006), 1822 (2008) and 1904 (2009) of the United Nations Security Council regarding sanctions against the members of the Alqaida organization, Usama bin Laden and the Taliban and other individuals, groups, undertakings and entities associated with them

ANNEX II Anti Money Laundering and Terrorist Financing Law

CHAPTER I

GENERAL PROVISIONS

Subject Matter of the Law

Article 1

(1) This Law shall prescribe:
1. measures and actions in banking and non-banking financial operations, money-related and other operations taken for the purpose of the prevention and detection of money laundering and terrorist financing;
2. reporting entities subject to this Law obliged to implement the measures and actions;
3. supervision over reporting entities in their implementation of measures and actions in banking and non-banking financial operations, cash and other operations, which measures and actions shall be taken for the purpose of money laundering and terrorist financing prevention and detection;
4. tasks and jurisdictions of the Anti-Money Laundering Office (hereinafter referred to as the Office) acting as a Financial Intelligence Unit;
5. international co-operation of the Office;
6. jurisdictions and actions of other state bodies and legal persons with public authorities in the detection of money laundering and terrorist financing;
7. other issues of significance for the development of the preventive system within the scope of money laundering and terrorist financing prevention.

(2) The provisions contained in this Law pertinent to the money laundering prevention shall equally adequately apply to the countering of terrorist financing for the purpose of preventing and detecting activities of individuals, legal persons, groups and organisations in relation with terrorist financing.

Basic Terms

Article 2

Basic terms in the context of this Law shall mean as follows:

1) money laundering shall mean the undertaking of actions aimed at concealing the true source of money or other property suspected to have been obtained in an illegal manner in the country or abroad, including:
   - conversion or any other transfer of money or other such property;
   - the concealment of the true nature, source, location, disposition, movement, ownership or rights with respect to money or other such property;
   - the acquisition, possession or use of money or other such property.
2) The terrorist financing shall mean the provision or collection of, as well as an attempt to provide or collect legal or illegal funds by any means, directly or indirectly, with the intention that they should be or in the knowledge that they are to be used, in full or in part, in order to carry out a terrorism offence by a terrorist or by a terrorist organisation.

Meaning of other Terms

Article 3

Other terms in the context of this Law shall have the following meaning:
1. The Office shall be the Anti-Money Laundering Office;
2. Financial Intelligence Unit:

a) the Anti-Money Laundering Office shall be the domestic Financial Intelligence Unit;
b) a foreign financial intelligence unit shall be a central national body in charge of receiving, analysing and disseminating suspicious transactions reports relating to money laundering and financing of terrorism in a member-state or a third country;

3. A member-state shall be a European Union member-state or a state signatory to the European Economic Area Agreement;
4. A third country shall be a European Union non-member state or a state non signatory to the European Economic Area Agreement.
5. Property shall be assets of every kind, whether tangible or intangible, movable or immovable, and documents and instruments in any form, including electronic or digital, evidencing title to or ownership rights in relation to the assets;
6. Funds shall be financial resources and benefits of any kind, including the following:
   a) cash, cheques, cash claims, bills of exchange, cash remittances and other means of payment;
   b) fund invested with reporting entities;
   c) securities as defined in the law providing for the securities market being traded through public or private offers, including shares and stakes, certificates, debt instruments, bonds, guarantees and derived financial instruments;
   d) other documents evidencing rights over financial resources or other financial sources;
   e) interest, dividends and other capital gains;
   f) accounts receivable, loans and letters of credit.
7. Reporting entities shall be legal and natural persons who shall be under obligation to undertake measures and actions for the purpose of preventing and detecting money laundering and terrorist financing in keeping with this Law;
8. An authorised person and his/her deputy shall be persons appointed by the reporting entity, authorised and responsible for implementation of measures and actions being undertaken for the purpose of money laundering and terrorist financing prevention and detection, as prescribed in this Law and regulations passed on the basis of this Law;
9. Persons involved in the performance of professional activities shall be legal and natural persons acting within the framework of their respective professional activities, including lawyers, law firms, notaries public, auditing firms, independent auditors, legal and natural persons involved in the performance of accounting services and tax advisory services;
10. Other legal persons, i.e. the entities made equal to them shall be NGOs, endowments and foundations and other legal persons not engaged in an economic activity, as well as religious communities and NGOs without legal personality and other entities without legal personality but appearing autonomously in legal transactions;
11. The electronic money and electronic data carrier shall bear the same meanings as provided for in regulations dealing with electronic operations;
12. The credit institution shall be a notion applicable to the reporting entities referred to in Article 4, paragraph 2, item 1, 2, 3 and 11 within the same meaning as defined in the law providing for the operations of credit institutions;
13. The financial institution shall be a notion applicable to reporting entities referred to in Article 4, paragraph 2, items 4, 5, 7, 8, 9, 10, 12, 15 a) to i) of this Law and the institutions of member-states dealing with the equal matters as the said reporting entities;
14. A business relationship shall be any business or other contractual relationship a customer establishes or enters into with a reporting entity and in relation to the performance of reporting entity's business activity;
15. Cash referred to in Article 40 of this Law shall be banknotes and coins in circulation as legal means of payment;
16. Cash referred to in Article 74 of this Law shall bear the same meaning as laid down in the Regulation of the European Parliament and of the Council (EC) No.1889/2005 as of 26 October 2005 on controlling cash entering or leaving the European Union;
17. Transaction account or a payment operations conducting account shall bear the same meaning as laid down in the law providing for the payment operations services;
18. A transaction shall be any receipt, outlay, transfer between accounts, conversion, keeping,

disposition and other dealings with money or other property with a reporting entity;

19. A cash transaction shall be any transaction in which a reporting entity should receive cash from a customer, i.e. hand over cash to and for customer's possession and disposal;
20. A suspicious transaction shall be any transaction for which the reporting entity and/or a competent body shall deem that there shall be reasons for suspicion of money laundering or terrorist financing in relation to the transaction or a person conducting the transaction, i.e. a transaction suspected to involve resources from illegal activities;
21. Trusts and company service providers shall be any legal or natural person whose business activity shall consist of the provision of some of the services listed hereunder on behalf of third parties:
    a) foundation of a legal person;
    b) performing the role of a Chief Executive Officer or a board member or enabling a third party to perform the role of a Chief Executive Officer or a board member, a manager or a partner, while such an undertaking does not involve the actual performance of a managerial function, i.e. such person does not assume business risk in relation to capital interest in the legal person in which the person shall formally be a member or a partner;
    c) providing a legal person with a registered seat or a rented business, postal or administrative address and other related services;
    d) performing the role or enabling another person to perform the role of a manager of an institution, a fund or similar legal entity subject to foreign law which receives, manages or distributes economic benefits for a purpose, whereby the definition shall exclude investment and pension funds management companies;
    e) using or enabling another person to use other people's shares for the purpose of exercising voting rights, except if it includes a company whose securities are being traded on a stock exchange or the regulated public market, for which
    disclosure requirements shall be in effect in keeping with the European Union regulations or international standards;
22. Companies performing certain payment operations services, including money transfers, shall be legal persons who perform financial services of receiving cash, cheques or other means of payment at one location and then executing disbursements of an adequate amount of money in cash or other form to a recipient at another location through connecting, notifying, transferring or using a money or values transfer network. Transaction being performed via such services may involve one or more intermediaries and final disbursement to a third party;
23. Non-profit organisations shall be associations, endowments, foundations, religious communities and other persons which do not perform economic activity;
24. The notion of a beneficial owner shall stand for:
    a) a natural person who is the ultimate owner of a customer or who controls or otherwise manages the legal person or other entity (if the customer is a legal person) or
    b) a natural person who shall control another natural person on whose behalf a transaction is being executed or who performs an activity (if the customer is a natural person);
25. Customer identification shall be a procedure involving:
    a) collection of information on customers on the basis of credible, independent and objective sources, i.e. examining the collected information on customers should the customer information have already been collected earlier;
    b) determining of actual customer identity on the basis of credible, independent and reliable sources, i.e. examining the identicalness thereof, should customer's identity have already been determined earlier.
26. A correspondent relationship shall be a relationship between a domestic credit institution and a foreign credit, i.e. other institution established by the opening of an account of the foreign institution with the domestic credit institution;
27. A shell (virtual) bank shall be a bank, i.e. other credit institution doing identical business activity registered in the country in which it does not perform its business activity and which is not related with a supervised or otherwise controlled financial group;
28. Factoring shall be the repurchase of accounts receivable with or without regress;
29. Forfeiting shall be an export financing on the basis of a discounted and regress free repurchase of long-term outstanding accounts receivable, secured through a financial instrument;

30. An official personal document shall be any public document with a photograph of a person issued by a domestic or a foreign competent public authority intended for establishing person's identity;
31. Stock exchange and the regulated public market notions shall bear the same meaning as laid down in the law providing for capital market;
32. The life insurance business shall be all business undertakings which are defined as such in laws providing for the insurance companies' operations;
33. Information on the activity of a customer who is a natural person shall be information on private or professional status (employed, pensioner, student, unemployed, etc.), i.e. information on the activity of a customer (in the fields of sports, culture-art, scientific-research, education or other related fields) representing grounds for the creation of a business relationship;
34. Foreign politically exposed persons shall be all natural persons with permanent address or habitual residence in a foreign country who act or have acted during the previous year (or longer) in a prominent public duty, including members of their immediate family or persons known to be close associates of such persons;
35. A money laundering or terrorist financing risk shall be the risk whereby a customer may abuse financial system for money laundering or terrorist financing purpose, i.e. that a business relationship, a transaction or a product shall be directly or indirectly used for money laundering or terrorist financing purposes.

Reporting Entities

Article 4

(1) Measures, actions and procedures for the prevention and detection of money laundering and terrorist financing laid down in this Law shall be carried out before and/or during each transaction, as well as upon entering into legal arrangements aimed at obtaining or using property and in other forms of disposing of monies, rights and other property in other forms which may serve for money laundering and terrorist financing purposes.

(2) Reporting entities obliged to carry out measures and actions referred to in paragraph 1 of this Article shall be:

1. banks, branches of foreign banks and banks from member-states authorised for a direct provision of banking services in the Republic of Croatia;
2. savings banks;
3. housing savings banks;
4. credit unions;
5. companies performing certain payment operations services, including money transfers;
6. Croatian Post Inc.
7. investment funds management companies, business units of third countries management companies, management companies from member-states which have a business unit in the Republic of Croatia, i.e. which are authorised to directly perform funds management business in the territory of the Republic of Croatia and third parties which are allowed, in keeping with the law providing for the funds operation, to be entrusted with certain matters by the respective management company;
8. pension companies;
9. companies authorised to do business with financial instruments and branches of foreign companies dealing with financial instruments in the Republic of Croatia;
10. insurance companies authorised for the performance of life insurance matters, branches of insurance companies from third countries authorised to perform life insurance matters and insurance companies from member-states which perform life insurance matters directly or via a branch in the Republic of Croatia;
11. companies for the issuance of electronic money, branches of companies for the issuance of electronic money from member-states, branches of companies for the issuance of electronic money from third countries and companies for the issuance of electronic money from

member-states authorised to directly render services of issuing electronic money in the Republic of Croatia;

12. authorised exchange offices;
13. organisers of games of chance:
    a) lottery games,
    b) casino games,
    c) betting games,
    d) slot-machine gaming,
    e) games of chance on the Internet and via other telecommunications means, i.e. electronic communications;
14. pawnshops;
15. legal and natural persons performing business in relation to the activities listed hereunder:
    a) giving credits or loans, also including: consumers' credits, mortgage loans, factoring and commercial financing, including forfeiting,
    b) leasing,
    c) payment instruments issuance and management (e.g., credit cards and traveller's cheques),
    d) issuance of guarantees and security instruments,
    e) investment management on behalf of third parties and providing advisory thereof,
    f) rental of safe deposit boxes,
    g) credit dealings intermediation,
    h) insurance agents with entering into life insurance agreements,
    i) insurance intermediation with entering into life insurance agreements,
    j) trusts or company service providers,
    k) trading precious metals and gems and products made of them,
    l) trading artistic items and antiques,
    m) organising or carrying out auctions,
    n) real-estate intermediation.
16. legal and natural persons performing matters within the framework of the following professional activities:
    a) lawyers, law firms and notaries public,
    b) auditing firms and independent auditors,
    c) natural and legal persons performing accountancy and tax advisory services.

(3) Reporting entities referred to in paragraph 2, item 16 of this Article shall carry out measures for the prevention and detection of money laundering and terrorist financing as provided for in this Law in keeping with the provisions governing the tasks and duties of other reporting entities, unless otherwise prescribed in the third chapter of this Law.

(4) The Minister of Finance may issue a rulebook to set terms and conditions under which the reporting entities referred to in paragraph 2 of this Article who perform financial activities only occasionally or within a limited scope and with which there is a negligible money laundering or terrorist financing risk may be excluded from the group of reporting entities obliged to implement measures as per this Law.

(5) Branches of foreign credit and financial institutions and other reporting entities established in the Republic of Croatia as per a law providing for their work, in addition to branches of credit and financial institutions referred to in paragraph 2, items 1, 7, 9, 10, 11 of this Article, shall be reporting entities obliged to implement measures and actions referred to in paragraph 1 of this Article.

Obligation of reporting entities concerning the implementation of money laundering and terrorist financing prevention and detection measures in business units and companies seated in

third countries in majority ownership or with predominant decision-making rights exercised by the reporting entities

Article 5

(1) Reporting entities shall be obliged to ensure that money laundering and terrorist financing prevention and detection measures as prescribed by this Law are applied within the equal scope in their business units and companies in their majority ownership or with predominant decision-making rights, seated in a third country, unless such a course of action would be in direct contradiction to the legal regulations of the third country.

(2) Where the legislation of the third country does not permit the application of the money laundering and terrorist financing prevention and detection measures within the scope prescribed by this Law, the reporting entities shall be obliged to inform the Office of the matter without any undue delay and to institute adequate measures for the elimination of the money laundering or terrorist financing risk.

(3) Reporting entities shall be obliged to regularly inform their business units and companies in their majority ownership or in which they shall have predominant decision-making rights, seated in a third country, of internal procedures pertinent to money laundering and terrorist financing prevention and detection, especially in terms of customer due diligence, supply of data and information, keeping records, internal control and other significant circumstance related with the money laundering and terrorist financing prevention and detection.

CHAPTER II

MEASURES TAKEN BY THE REPORTING ENTITIES FOR THE PURPOSE OF MONEY LAUNDERING AND TERRORIST FINANCING PREVENTION AND DETECTION

Section 1

GENERAL PROVISIONS

Reporting Entities Duties

Article 6

(1) For the purpose of money laundering and terrorist financing prevention and detection, the reporting entities shall be obliged to fulfil the duties as provided for in this Law and regulations passed on the basis of this Law during the course of the performance of their regular activities.

(2) The duties referred to in the previous paragraph of this Article shall encompass as follows:

1. assessment of risk of abuse in relation with money laundering and terrorist financing specific to a customer, business relationship, transaction or a product;
2. carrying out customer due diligence measures in the manner and under the conditions provided by this Law;
3. conducting money laundering and terrorist financing prevention and detection measures in business units of the reporting entity and companies in which the reporting entity shall hold majority stake or predominant decision-making rights, which business units and companies shall be seated in third countries;
4. appointment of an authorised person and his/her deputy for implementing measures and ensuring adequate conditions for their work as per this Law and regulations passed on the basis of this Law;
5. enable regular professional training and education of employees of the reporting entities, and ensure regular internal audit in the execution of tasks and duties as per this Law and regulations passed on the basis of this Law;

6. produce and regularly update a list of indicators for the detection of customers and suspicious transactions for which there are reasons for suspicion of money laundering or terrorist financing;
7. reporting and supply of the prescribed and required data, information and documentation on transactions and persons to the Office in agreement with the provisions contained in this Law and regulations passed on the basis of this Law;
8. ensure data storage and protection and keeping the prescribed records as per this Law and regulations passed on the basis of this Law;
9. obligation of credit and financial institutions concerning the establishment of an adequate information system relevant for their respective organisational structures in order to be able to promptly, timely and completely provide the Office with data as to whether or not they shall maintain or have maintained a business relationship with a given natural or legal person, as well as to the nature of such a relationship;
10. carrying out other tasks and duties in keeping with this Law and regulations passed on the basis of the Law.

Assessment of Money Laundering or Terrorist Financing Risks

Article 7

(1) A money laundering or terrorist financing risk shall be the risk whereby a customer may abuse financial system for money laundering or terrorist financing purpose, i.e. that a business relationship, a transaction or a product shall be directly or indirectly used for money laundering or terrorist financing purposes.

(2) Reporting entities shall be obliged to develop a risk analysis and apply it to rate risks of individual groups or types of customers, business relationships, products or transactions in respect of possible abuse relative to money laundering and terrorist financing.

(3) Reporting entities shall undertake to align the risk analysis and assessment referred to in paragraph 2 with the guidelines to be passed by the competent supervisory bodies referred to in Article 83 of this Law in line with the powers vested in them.

(4) During the course of risk analysis and assessment, i.e. the procedure aimed at determining risk rating referred to in paragraph 2 of this Article, the reporting entity and the supervisory body referred to in Article 83 of this Law shall be obliged to take account of the specificities of the reporting entity and its operations, e.g. the reporting entity's size and composition, scope and type of business matters performed, types of customers it deals with and products it offers.

(5) The reporting entities may include only those customers meeting the requirements to be set forth in a rulebook to be passed by the Minister of Finance in the group of customers representing a negligible money laundering or terrorist financing risk.

Section 2

CUSTOMER DUE DILIGENCE

Customer Due Diligence Measures

Article 8

(1) Unless otherwise prescribed in this Law, customer due diligence shall encompass the following measures:

1. identifying the customer and verifying the customer's identity on the basis of documents, data or information obtained from a credible, reliable and independent source;

2. identifying the beneficial owner of the customer and verifying beneficial owner's identity;
3. obtaining information on the purpose and intended nature of the business relationship or transaction and other data in line with this Law;
4. conducting ongoing monitoring of the business relationship including due scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the reporting entity's knowledge of the customer, the type of business and risk, including, as necessary, information on the source of funds, in which the documents and data available to the reporting entity must be kept up-to-date.

(2) The reporting entities shall be obliged to define the procedures for the implementation of measures referred to in paragraph 1 in their respective internal enactments.

Obligation of Applying Customer Due Diligence Measures

Article 9

(1) Under the conditions laid down in this Law, the reporting entities shall be obliged to conduct customer due diligence in the following cases:

1. when establishing a business relationship with a customer;
2. when carrying out each transaction amounting to HRK 105,000.00 or more, whether the transaction is carried out in a single operation or several transactions which clearly appear to be linked and reaching a total value of HRK 105,000.00 or more;
3. when there are doubts about the credibility and veracity of the previously obtained customer or customer beneficial owner information;
4. in all instances when there are reasons for suspicion of money laundering or terrorist financing in relation to a transaction or a customer, regardless of the transaction value.

(2) With transactions referred to in paragraph 1, item 2 of this Article performed on the basis of a previously established business relationship with the reporting entity, in conducting customer due diligence the reporting entity shall only verify the identity of the customer, i.e. the persons who perform the transaction, and shall collect any missing information as referred to in Article 25, paragraph 2 of this Law.

Customer Due Diligence when Establishing a Business Relationship

Article 10

(1) In establishing a business relationship with a customer, the reporting entities shall be obliged to conduct the measures referred to in Article 8, paragraph 1, items 1, 2 and 3 of this Law before the establishment of the business relationship.

(2) By way of derogation from the provisions of the previous paragraph of this Article, the reporting entities may also conduct the measures referred to in Article 8, paragraph 1, items 1 and 2 of this Law during the establishment of a business relationship with a customer, should it be necessary not to interrupt the usual manner of establishing business relationships and if pursuant to Article 7 of this Law there is a negligible risk of money laundering or terrorist financing.

(3) By way of derogation from the provisions of paragraph 1 of this Article, the reporting entities referred to in Article 4, paragraph 2, item 10 of this Law may when concluding life insurance dealings identify the beneficiary under the insurance policy even after entering into an insurance contract, but no later than before or at the time of payout of the insured amount, i.e. at the point when the insurance right-holder requires the payout of the receipt, announces the intention of obtaining a loan on the basis of the policy, giving it as collateral or capitalising on it.

Customer Due Diligence when Carrying out a Transaction

Article 11

When carrying out transactions referred to in Article 9, paragraph 1, item 2 of this Law, the reporting entities shall be obliged to conduct measures prescribed in Article 8, paragraph 1, items 1, 2 and 3 before the carrying-out of the transaction.

Obligation of Applying Customer Due Diligence Measures by Organisers of Lottery Games, Casino Games, Betting Games, Games of Chance on Slot-Machines and Games of Chance on the Internet or other Telecommunication Means, i.e. Electronic Communications

Article 12

(1) Organisers of casino games shall conduct the measure of identifying the customer and verifying the customer's identity on customer's entry into the casino, collecting the following information:

- name and surname of natural person, permanent address, date and place of birth;
- identification number and name, number and name of the body which issued the identification document;
- date and time of entry into the casino.

(2) With the transaction referred to in Article 9, paragraph 1, item 2 of this Law, the organisers of lottery games, casino games, betting games and games of chance on slot machines shall identify the customer and verify the identity of the customer at the point of performing the transaction at the cash register, collecting the following information:

- name and surname of natural person, permanent address, date and place of birth;
- identification number and name, number and name of the body which issued the identification document;

(3) By way of derogation from the provisions contained in paragraph 2 of this Article, the organiser of lottery games, casino games, betting games and games of chance on slot machines shall be obliged to carry out due diligence measures when there are reasons for suspicion of money laundering or terrorist financing in relation with a customer, product or transaction, even for transactions amounting to HRK 105,000.00 and less on executing the transaction at the cash register.

(4) The establishment of a business relationship referred to in Article 9, paragraph 1, item 1 of this Law shall also include the registration of a customer to take part in the system of organising games of chance with organisers arranging the games of chance on the Internet or other telecommunications means, i.e. electronic communications.

(5) At establishing business relationship referred to in Article 9, paragraph 1, item 1 of this Law, the organiser of games of chance on the Internet or other telecommunications means, i.e. electronic communications, shall collect information referred to in paragraph 2 of this Article.

Refusing a business relationship and the conducting of a transaction

Article 13

(1) The reporting entity which is unable to conduct measures referred to in Article 8, paragraph 1, items 1, 2 and 3 of this Law shall not be allowed to establish a business relationship or to carry out a transaction, i.e. such a reporting entity must terminate the already established business relationship.

(2) In the cases referred to in paragraph 1 of this Article, the reporting entity shall notify the Office of the refusal or termination of a business relationship and the refusal to conduct a transaction with all customer of transaction data collected to date in line with Article 42 of this Law.

Exemptions from Conducting Due Diligence Measures for Some Products

Article 14

(1) Insurance companies licensed for the performance of life insurance business, the business units of insurance companies from third countries licensed for the performance of life insurance business, insurance companies from member-states which are to establish a business unit in the Republic of Croatia or are authorised to directly perform life insurance business in the Republic of Croatia, pension companies, as well as legal and natural persons performing business or activity of insurance representation or intermediation for entering into life insurance agreements, may be allowed not to conduct the customer due diligence measures under the following circumstances:

1. with contracting life insurance policies in which individual premium instalment or several insurance premium instalments to be paid within one year does not exceed a total kuna equivalent amount of EUR 1,000.00 or in cases when single premium payment does not exceed the kuna equivalent value of EUR 2,500.00;

2. with contracting pension insurances providing that:

   a) types of insurance are being contracted whereby it is not possible to transfer the insurance policy to a third person or use it as collateral for a credit or loan, and
   b) a contract is entered into with a closed-end pension fund if the employer pays the contributions into the voluntary pension fund on behalf of the fund's members.

(2) Companies for the issuance of electronic money, companies for the issuance of electronic money from another member state and business units of foreign companies for the issuance of electronic money may be allowed not to conduct customer due diligence measures in the following instances:

1. with issuing electronic money, if the single amount of payment executed for the issuance of such a money, on an electronic data carrier which may not be recharged, does not exceed kuna equivalent value totalling EUR 150.00;
2. with issuing electronic money and performing business with it if the total amount of the executed payments, stored on an electronic data carrier which may be recharged, does not exceed kuna equivalent value totalling EUR 2,500.00 during the current calendar year, save for cases in which the holder of electronic money cashes out a kuna equivalent amount of EUR 1,000.00 or more during the same calendar year.

(3) The Minister of Finance may issue a rulebook to prescribe that a reporting entity may be excluded from the obligation of conducting customer due diligence when conducting certain transactions referred to in Article 9, paragraph 1, item 2 of this Law and in respect of other products and transactions associated with them, which shall represent a negligent money laundering or terrorist financing risk.

(4) By way of derogation from the provisions contained in paragraphs 1, 2 and 3 of this Article, the exclusion from conducting customer due diligence in respect of a customer, product or transaction shall not be allowed when there are reasons for suspicion of money laundering or terrorist financing.

Wire transfers

Article 15

(1) Credit and financial institutions, including companies involved in certain payment operations services or money transfers (hereinafter referred to as the payment service providers) shall be obliged to collect accurate and complete data on the payer and include them in a form or a message accompanying the wire transfer, sent or received in any currency. In doing so, data must follow the transfer at all times throughout the course of the chain of payment.

(2) The Minister of Finance shall issue a rulebook to prescribe content and type of data to be collected on the payer and other obligations of the payment service providers and exceptions from the

obligation of collecting data at money transfers representing a negligible money laundering or terrorist financing risk.

(3) The payment service provider, which shall act as intermediaries or cash receivers, shall refuse wire transfers failing to contain complete data on the payer referred to in paragraph 2 of this Article or shall ask for payer data supplement within a given deadline.

(4) The payment service providers may restrict or terminate a business relationship with those payment service providers who frequently fail to meet the requirements referred to in paragraphs 1 and 2 of this Article, with that they may alert them on such a course of action before taking such measures. The payment service provider shall notify the Office of a more permanent restriction or business relationship termination.

(5) The payment service provider, which shall act as intermediaries or cash receivers, shall consider a lack of payer information in relation to the assessed level of risk as a possible reason for implementing enhanced transactions due diligence measures, and shall adequately apply provisions contained in Article 43, paragraphs 2 and 3 of this Law.

(6) The provisions contained in paragraphs 1 to 5 of this Article shall pertain to wire transfers conducted by both domestic and foreign payment service providers.

(7) When gathering data referred to in the Paragraph 1 of this Article, the payment service providers shall identify the payer by using an official identification document, and credible and reliable sources of documentation.

Section 3

CONDUCTING CUSTOMER DUE DILIGENCE MEASURES

Obtaining Information from the Reporting Entities

Article 16

(1) During the course of conducting customer due diligence, the reporting entities referred to in Article 4, paragraph 2 shall obtain the following data:

1. name and surname, permanent address, date of birth, place of birth, personal identification number, name and number of the identification document issuing entity for the following natural persons:
   - natural person and natural person's legal representative, a craftsman or a person involved in carrying out other independent business activity, who shall establish a business relationship or conduct a transaction, i.e. on whose behalf the business relationship is being established or a transaction conducted;
   - legal representative or a person authorised by power of attorney who shall establish a business relationship or conduct a transaction on behalf of the legal person or another legal person and entity made equal to it from Article 21 of this Law;
   - person authorised by poser of attorney requesting or conducting a transaction for a customer;
   - a natural person, a craftsman or a person carrying out other independent business activity, for whom the lawyer, the law firm and the notary public, and the auditing company, the independent auditor, legal and natural persons involved in the performance of accounting services and tax advisory services shall conduct business matters;
   - a natural person in relation to whom there shall be reasons for suspicion of money laundering or terrorist financing, which reasons shall be established by a lawyer, a law firm and a notary public, and an auditing firm, an independent auditor, legal and natural persons involved in the performance of accounting services and tax advisory services;
2. name and surname, permanent address, date of birth, place of birth for the following natural persons:

- natural person approaching a safe deposit box;
- natural person who is a member of another legal person and an entity related to it as referred to in Article 21 of this Law;

3. name, surname and permanent address for:
   - natural person to whom the transaction shall be intended;
4. name and surname, permanent address, date of birth and place of birth of the beneficial owner;
5. name, seat (street and number, place and country) and business registration number (for a legal person, whereas the registration number is to be included for a craftsman or a person carrying out other independent business activity if such a number has been assigned to such a person) for:
   - a legal person establishing a business relationship or conducting a transaction, i.e. a legal person on whose behalf a business relationship is being established or transaction conducted;
   - craftsman or a person carrying out other independent business activity;
   - a legal person for whom a lawyer, a law firm, a notary public, an auditing firm, an independent auditor, legal and natural persons involved in the performance of accounting services and tax advisory services shall conduct business matters;
   - a craftsman or a person carrying out other independent business activity for whom a lawyer, a law firm, a notary public, an auditing firm, an independent auditor, legal and natural persons involved in the performance of accounting services and tax advisory services shall conduct business matters;
   - a legal person in relation to which there shall be reasons for suspicion of money laundering or terrorist financing, which reasons shall be established by a lawyer, a law firm and a notary public, and an auditing firm, an independent auditor, legal and natural persons involved in the performance of accounting services and tax advisory services;
6. name and seat for:
   - a legal person or a craftsman to whom the transaction shall be intended;
   - other legal persons and entities made equal to them as referred to in Article 21 of this Law
7. information on the purpose and intended nature of the business relationship, including information on customer's business activity;
8. date and time of:
   - establishing a business relationship;
   - approaching a safe deposit box;
9. date and time of conducting a transaction, the transaction amount and currency in which the transaction is being executed, purpose (intention) of the transaction, the manner of transaction execution;
10. information on the source of funds, which are or will be subject matter of a business relationship or a transaction;
11. reasons for suspicion on money laundering or terrorist financing.

(2) The Minister of Finance may issue a rulebook to prescribe additional data the reporting entities shall be obliged to supply for the purposes of due diligence and reporting the Office on transactions.

Sub-section 1

MEASURE OF IDENTIFYING THE CUSTOMER AND VERIFYING THE CUSTOMER'S IDENTITY

Identifying a Natural Person and Verifying the Natural Person's Identity

Article 17

(1) For a customer which is a natural person and natural person's legal representative, and for a customer who is a craftsman or a person involved in the performance of another independent business activity, the reporting entity shall identify the customer and verify the customer's identity through the collection of data referred to in Article 16, paragraph 1, item 1 of this Law through the examination of official customer's personal identification document in customer's presence.

(2) Should the reporting entity be unable to collect the prescribed data from the official personal identification document submitted, the missing data shall be collected from other valid public documents submitted by the customer, i.e. directly from the customer.

(3) The reporting entity may identify the customer and verify the customer's identity in cases when the customer is a natural person, i.e. the person's legal representative, a craftsman and a person involved in the performance of other independent business activity in other ways, should the Minister of Finance prescribe so in a rulebook.

(4) In instances in which the customer is a craftsman or a person involved in the performance of other independent business activity, the reporting entity shall collect data defined in Article 16, paragraph 1, item 5 of this Law in keeping with the provisions contained in Article 18 of this Law.

(5) Should the reporting entity have suspicion during the course of identifying the customer and verifying the customer's identity in accordance with the provisions of this Article as to the veracity of data collected or credibility of the documents and other business documentation from which data was collected, the reporting entity is to also require the customer to give a written statement.

Identifying a Legal Person and Verifying the Legal Person's Identity

Article 18

(1) For a customer who is a legal person, the reporting entity shall identify the customer and verify the customer's identity through the collection of data referred to in Article 16, paragraph 1, item 5 of this Law by examining the original or notarised photocopy of documentation from court or other public register presented by the legal person's legal representative or person authorised by power of attorney.

(2) At the time of submission, the documentation referred to in paragraph 1 must not be more than three months old.

(3) The reporting entity may identify the legal person and verify the legal person's identity through the collection of data referred to in Article 16, paragraph 1, item 5 of this Law through a direct examination of court or other public register. On the excerpt from the register examined, the reporting entity shall put date, time, name and surname of the examiner. The reporting entity shall keep the excerpt from the register in keeping with the provisions of this Law concerning data protection and keeping.

(4) The reporting entity shall collect other data referred to in Article 16, paragraph 1 of this Law, save for data on beneficial owner, through the examination of original or notarised photocopies of documents and other business documentation. Should the documents and documentation referred to be insufficient to enable the collection of all data from Article 16, paragraph 1 of this Law, the reporting entity shall collect the missing data, save for data on beneficial owner, directly from the legal representative or the person authorised by power of attorney.

(5) Should the reporting entity have any suspicion during the course of identifying the legal person and verifying the legal person's identity as to the veracity of data collected or credibility of the documents and other business documentation from which data was collected, the reporting entity is to also require the legal representative or the person authorised by power of attorney to give a written statement prior to the establishment of a business relationship or execution of a transaction.

(6) While verifying customer's identity on the basis of paragraphs 1 and 3 of this Article, the reporting entity must first check the nature of a register from which the reporting entity shall take data for the identity verification purposes.

(7) Should the customer be a legal person performing business activity in the Republic of Croatia through its business unit – a branch, the reporting entity shall identify the foreign legal person and its branch and verify their respective identities.

Identifying a legal person's legal representative and verifying the legal representative's identity

Article 19

(1) The reporting entity shall identify a legal person's legal representative and verify the legal representative's identity through the collection of data referred to in Article 16, paragraph 1, item 1 of this Law through examination of a personal identification document of the legal representative in his/her presence. Should the document be insufficient to enable the collection of all prescribed data, the missing data shall be collected from other valid public document proposed by the customer, i.e. supplied by the legal representative.

(2) Should the reporting entity have any suspicion during the course of identifying the legal representative and verifying the legal representative's identity as to the veracity of the collected data, the reporting entity is to also require the legal representative to give a written statement.

Identifying a legal or natural person's person authorised by power of attorney and verifying the identity of the person authorised by power of attorney

Article 20

(1) Should a person authorised by power of attorney be establishing a business relationship on behalf of a legal person instead of the legal person's legal representative referred to in Article 19 of this Law, the reporting entity shall identify the person authorised by power of attorney and verify such person's identity by collecting data provided for in Article 16, paragraph 1, item 1 of this Law through the examination of an official personal identification document of the person authorised by power of attorney in his/her presence.

(2) Should the document be insufficient to enable the collection of all prescribed data, the missing data shall be obtained from other valid public document submitted by the person authorised by power of attorney, i.e. directly from this person. The reporting entity shall collect data referred to in Article 16, paragraph 1, item 1 of this Law on the legal representative who issued a power of attorney on behalf of the legal person on the basis of data included in the notarised power of attorney.

(3) Should a person authorised by power of attorney conduct transactions referred to in Article 9, paragraph 1, item 2 of this Law on behalf of a customer who is a legal person, a natural person, a craftsman or a person involved in the performance of other independent business activity, the reporting entity shall identify the person authorised by power of attorney and verify such person's identity via the collection of data referred to in Article 16, paragraph 1, item 1 of this Law.

(4) The reporting entity shall collect data referred to in Article 16, paragraph 1, items 1 and 5 of this Law on the customer on whose behalf the person authorised by power of attorney shall act, which data shall be collected on the basis of the notarised power of attorney.

(5) Should the reporting entity have suspicion during the course of identifying the person authorised by power of attorney and verifying such person's identity as to the veracity of the collected data, the reporting entity is to also require the person's written statement.

Identifying other legal persons and entities made equal to them and verifying their respective identities

Article 21

(1) In cases of NGOs, endowments and foundations and other legal persons who do not perform economic activity, as well as in cases of religious communities and NGOs without properties of a legal person and other entities without legal personality but independently appearing in legal transactions, the reporting entities shall be obliged to:

1. identify the person authorised to represent, i.e. a representative and verify representative's identity;
2. obtain a power of attorney for representation purposes;
3. collect data referred to in Article 16, paragraph 1, items 1, 2 and 6 of this Law.

(2) The reporting entity shall identify the representative and verify the representative's identity referred to in paragraph 1 of this Article via the collection of data referred to in Article 16, paragraph 1, item 1 of this Law through the examination of an official personal identification document of the representative in his/her presence. Should the document be insufficient to collect all prescribed data, the missing data shall be collected from other valid public document submitted by the representative, i.e. from the representative directly.

(3) The reporting entities shall collect data referred to in Article 16, paragraph 1, item 2 of this Law on each natural person who is a member of an NGO or other entity referred to in paragraph 1 of this Article from a power of attorney issued for representation purposes and submitted by the representative to the reporting entity. Should the authorisation be insufficient to enable the collection of all data referred to in Article 16, paragraph 1, item 2 of this Law, the missing data shall be collected from the representative directly.

(4) Should the reporting entity have suspicion during the course of identifying the person referred to in paragraph 1 of this Article and verifying such person's identity as to the veracity of the collected data or the credibility of documents from which data was collected, the reporting entity must also require the representative to give a written statement before the establishment of a business relationship or the execution of a transaction.

Special Customer Identification and Identity Verification Cases

Article 22

(1) For the purpose of implementing the provisions contained in Article 9 of this Law, identity of customers also must be established and verified on each customer's use of a safe deposit box.

(2) During the course of identifying customers on the basis of paragraph 1 of this Article and verifying such customers' identity, the reporting entity involved in business activity of safekeeping items in safe deposit boxes shall collect data referred to in Article 16, paragraph 1, item 2 of this Law.

(3) The provisions contained in this Article in respect of the obligation to identify a customer when using a safe deposit box shall pertain to all natural persons who actually use the safe deposit box, regardless of whether such a person is the actual user of the safe deposit box as per the safe deposit box use contract or such a person's legal representative or person authorised by power of attorney.

Sub-section 2

THE BENEFICIAL OWNER IDENTIFICATION MEASURE

Customer's Beneficial Owner

Article 23

(1) The beneficial owner shall be:

1. with legal persons, branches, representative offices and other entities subject to domestic and foreign law made equal with a legal person:
   - the natural person who ultimately owns or controls a legal entity through direct or indirect ownership or a natural person who controls a sufficient percentage of shares of voting rights in that legal person, and a percentage of 25 per cent plus one share shall be deemed sufficient to meet this requirement,
   - a natural person who otherwise exercises control over management of a legal person;

2. with legal persons, such as endowments and legal transactions such as trust dealings which administer and distribute monies:
   - where the future beneficiaries have already been determined, the natural person who is the beneficial owner of 25% or more of the property rights of the legal transaction,
   - where natural or legal persons who will benefit from the legal transactions have yet to be determined, the persons in whose main interest the legal transaction or legal person is set up or operates;
   - natural person who exercises control over 25% or more of the property rights of the legal transaction.
3. a natural person who shall control another natural person on whose behalf a transaction is being conducted or an activity performed.

Identifying Customer's Beneficial Owner

Article 24

(1) The reporting entity shall identify customer's beneficial owner which shall be a legal person, a representative office, a branch, another entity subject to domestic or foreign law made equal with a legal person through the collection of data prescribed in Article 16, paragraph 1, item 4 of this Law.

(2) The reporting entity shall collect data referred to in paragraph 1 of this Article through the examination of the original or notarised documents from a court or other public register, which may not be more than three months old.

(3) The reporting entity may collect data referred to in paragraph 1 of this Article also through direct examination of court or other public register while taking account of the provisions contained in Article 18, paragraphs 3 and 5 of this Law.

(4) Should the court or other public register be insufficient to enable the collection of data on customer's beneficial owner, the reporting entity shall collect the missing data through the examination of the original or notarised documents and other business documentation supplied to the reporting entity by the legal representative or person authorised by power of attorney.

(5) Should it arise that the missing data for objective reasons cannot be collected in the manner set forth in paragraphs 2, 3 and 4 of this Article, the reporting entity shall collect data directly from a written statement given by the customer's legal representative or the person authorised by power of attorney as referred to in paragraph 1 of this Article.

(6) The reporting entity must collect data on the ultimate beneficial owner of a customer referred to in paragraph 1 of this Article. The reporting entity shall check the collected data in the manner that enables the reporting entity to have knowledge of the ownership structure and control of the customer to an extent that meets the criterion of satisfactory knowledge of beneficial owners, depending on risk assessment.

Sub-section 3

MEASURE OF COLLECTING INFORMATION ON THE PURPOSE AND INTENDED NATURE OF THE BUSINESS RELATIONSHIP OR TRANSACTION, AND OTHER INFORMATION AS PER THIS LAW

Data collection

Article 25

(1) Within the framework of customer due diligence during the course of establishing a business relationship referred to in Article 9, paragraph 1, item 1 of this Law, the reporting entity shall collect information referred to in Article 16, paragraph 1, items 1, 4, 5, 7 and 8 of this Law.

(2) Within the framework of customer due diligence with each transaction totalling HRK 105,000.00 and more, regardless of whether the transaction is made as a single operation or as several transactions which clearly appear to linked as referred to in Article 9, paragraph 1, item 2 of this Law, the reporting entity shall collect information referred to in Article 16, paragraph 1, items 1, 3, 4, 5, 6 and 9 of this Law.

(3) Within the framework of customer due diligence in instances when there is suspicion as to the credibility and veracity of the previously collected information on customers or the beneficial owner, and in all instances when there are reasons to have suspicion of money laundering or terrorist financing associated with a transaction or a customer as referred to in Article 9, paragraph 1, items 3 and 4 of this Law, the reporting entity shall collect information referred to in Article 16, paragraph 1 of this Law.

Sub-section 4

MEASURE OF THE BUSINESS RELATIONSHIP MONITORING

Measure of Ongoing Monitoring of the Business Relationship

Article 26

(1) The reporting entity shall be obliged to exercise due care in monitoring of business activity the customer shall conduct with the reporting entity, thereby ensuring the knowledge of the customer, including the knowledge of the source of funds at customer's disposal for doing business. (2) The reporting entity shall be obliged to monitor business activities conducted by the customer with the reporting entity through the application of the following measures:

1. monitoring and scrutinising the compliance of customer's business with the intended nature and purpose of the business relationship the customer had established with the reporting entity;
2. monitoring and scrutinising the compliance of sources of funds with the intended source of funds the customer had indicated at the establishment of the business relationship with the reporting entity;
3. monitoring and scrutinising the compliance of customer's operations or transactions with the customer's usual scope of business operation or transactions;
4. monitoring and updating the collected documents and information on customers, including the carrying out of repeated annual customer due diligence in instances set forth in Article 27 of this Law.

(3) The reporting entity shall be obliged to ensure that the scope, i.e. the frequency of conducting measures referred to in paragraph 2 of this Article be adapted to the money laundering or terrorist financing risk to which the reporting entity shall be exposed during the course of conducting individual business undertakings, i.e. during the course of doing business with individual customers, in keeping with the provisions contained in Article 7 of this Law.

Repeated Annual Foreign Legal Person Due Diligence

Article 27

(1) Should a foreign legal person have a business relationship established or conduct transactions referred to in Article 9, paragraph 1, items 1 and 2 of this Law with a reporting entity, the reporting entity shall, in addition to the application of business activities monitoring measures laid down in Article 26 of this Law, be obliged to regularly at least once a year, and no later than after the expiration of one year since the last customer due diligence had been conducted, conduct the repeated annual foreign legal person due diligence.

(2) By way of derogation from the provisions contained in paragraph 1 of this Article, the reporting entity shall be obliged to regularly at least once a year, and no later than after the expiration of one year since the last customer due diligence had been conducted, carry out a repeated customer due diligence also when the customer, conducting transactions referred to in Article 9, paragraph 1, item 2 of this Law, shall be a legal person seated in the Republic of Croatia and with 25% and greater ownership stake held by:

1. a foreign legal person which does not perform or is not allowed to perform trading, production or other activities in the domicile country of registration;
2. a trust or other similar foreign law company with unknown, i.e. hidden owners, secret investors or managers.

(3) The repeated customer due diligence referred to in paragraphs 1 and 2 of this Article shall encompass:

1. gathering and scrutinising information on the name, address and seat of the foreign legal person from paragraphs 1 and 2 of this Article;
2. gathering and scrutinising information on the name, surname and permanent address of the foreign legal person's legal representative from paragraphs 1 and 2 of this Article;
3. gathering and scrutinising information on the beneficial owner of the foreign legal person from paragraphs 1 and 2 of this Article;
4. obtaining a new power of attorney referred to in Article 20, paragraph 4 of this Law.

(4) With the execution of transactions referred to in Article 9, paragraph 1, item 2 of this Law on behalf and for the account of a foreign legal person, i.e. its business unit, a branch or a representative office conducting the transactions with the reporting entity, the reporting entity shall gather information listed hereunder during the course of the repeated foreign legal person due diligence, in addition to the information set forth in paragraph 3 of this Article:

1. information on the address and seat of the foreign legal person's business unit;
2. information on name, surname and permanent address of the foreign legal person's business unit's legal representative.

(5) The reporting entity shall gather information referred to in paragraph 3, items 1, 2 and 3 of this Article via the examination of the original or notarised photocopies of documentation from court or other public register which documentation may not be more than three months old, i.e. via a direct examination of the court or other public register.

(6) Should the manner described in paragraph 5 of this Article be insufficient to allow the collection of all required information, the reporting entity shall collect the missing information from the original or notarised photocopies of documents and other business documentation supplied to the reporting entity by the foreign legal person referred to in paragraphs 1 and 2 of this Article.

(7) Should the missing information may not be collected in the prescribed manner for objective reasons, the reporting entity shall collect such information directly from a written statement given by the foreign legal person's legal representative referred to in paragraphs 1 and 2 of this Article.

(8) The reporting entity shall not be permitted to conduct transactions for a customer for which the reporting entity has not conducted or failed in conducting the repeated annual customer due diligence in keeping with this Article.

(9) By way of derogation from the provisions contained in paragraph 1 of this Article, the repeated annual foreign legal person due diligence shall not be required if the foreign legal person is a reporting entity referred to in Article 35, paragraph 1 of this Law.

Section 4

CUSTOMER DUE DILIGENCE THROUGH THIRD PERSONS

Entrusting a Third Party with Conducting Due Diligence

Article 28

(1) Under the conditions provided for in this Law, at establishing business relationship with a customer the reporting entity may entrust a third party with identifying the customer and verifying the customer's identity, identifying the beneficial owner of the customer, collecting information on the purpose and intended nature of the business relationship or a transaction in keeping with Article 8, paragraph 1, items 1, 2 and 3 of this Law.

(2) The reporting entity must first check whether or not the third party who shall be entrusted with the conducting of customer due diligence measures meets all requirements prescribed by this Law.

(3) The reporting entity shall not be permitted to accept customer due diligence conducted by a third party on behalf of the reporting entity as adequate, if the third party conducted the identification and identity verification measure within the due diligence exercise without customer's presence.

(4) Should it arise that a third person conducted customer due diligence in lieu of the reporting entity, such person shall also be accountable for meeting the obligations as per this Law, including the obligation of reporting on transactions in relation to which suspicion of money laundering or terrorist financing shall exist and the obligation of keeping data and documentation.

(5) The responsibility for conducting due diligence measures entrusted with a third party shall still rest with the reporting entity.

(6) The Minister of Finance shall prescribe in a rulebook who may be a third person, terms and conditions under which the reporting entities shall be allowed to entrust the conducting of customer due diligence with a third person, the manner in which the reporting entities shall be enabled to obtain data and documentation prescribed in this Law from a third person, and instances in which the reporting entities shall not be permitted to entrust a third person with conducting customer due diligence.

Section 5

SPECIAL FORMS OF CUSTOMER DUE DILIGENCE

General Provisions

Article 29

(1) Customer due diligence shall as a rule be conducted in keeping with the provisions contained in Article 8, paragraph 1 of this Law, whereas special forms of customer due diligence shall be carried out for cases defined by this Law, including:

1. enhanced customer due diligence;
2. simplified customer due diligence.

Sub-section 1

ENHANCED CUSTOMER DUE DILIGENCE

General Provisions

Article 30

(1) In addition to the measures referred to in Article 8, paragraph 1 of this Law, enhanced customer due diligence shall include additional measures provided for by this Law for the cases as follows:

1. the establishment of a correspondent relationship with a bank or other similar credit institution seated in a third country;
2. the establishment of a business relationship or the conducting of a transaction referred to in Article 9, paragraph 1, items 1 and 2 of this Law with a customer who is a politically exposed person as referred to in Article 32 of this Law;
3. in instances when the customer was not present in person during identification and identity verification of the person during the course of due diligence measures implementation.

(2) The reporting entity shall be obliged to conduct enhanced customer due diligence in all instances covered in paragraph 1 of this Article.

(3) The reporting entity may apply an enhanced customer due diligence measure or measures in other circumstances when it shall deem in accordance with the provisions of Article 7 of this Law that there shall exist or might exist a great degree of money laundering or terrorist financing risk, due to the nature of the business relationship, the form and manner of transaction execution, business profile of the customer or other circumstances associated with the customer.

Correspondent Relationships with Credit Institutions from Third Countries

Article 31

(1) At establishing a correspondent relationship with a bank or other credit institution seated in a third country, the reporting entity shall be obliged to conduct measures referred to in Article 8, paragraph 1 within the framework of enhanced customer due diligence and additionally gather the following data, information and documentation:

1. date of issuance and validity period of license for the performance of banking services, as well as the name and seat of the competent third country license issuing body;
2. description of the implementation of internal procedures relative to money laundering and terrorist financing prevention and detection, notably the procedures of customer identify verification, beneficial owners identification, reporting the competent bodies on suspicious transactions and customers, keeping records, internal audit and other procedures the respective bank, i.e. other credit institution passed in relation with money laundering and terrorist financing prevention and detection;
3. description of the systemic arrangements in the field of money laundering and terrorist financing prevention and detection in effect in the third country in which the bank or other credit institution has its seat or in which it was registered;
4. a written statement confirming that the bank or other credit institution does not operate as a shell bank;
5. a written statement confirming that the bank or other credit institution neither has business relationships with shell banks established nor does it establish relationships or conduct transactions with shell banks;
6. a written statement confirming that the bank or other credit institution falls under the scope of legal supervision in the country of their seat or registration, and that they are obliged to apply legal and other regulations in the field of money laundering and terrorist financing prevention and detection in keeping with the effective laws of the country.

(2) A reporting entity's employee involved in establishing correspondent relationships referred to in paragraph 1 of this Article and running the enhanced customer due diligence procedure shall be obliged to obtain a written consent from the superior responsible person of the reporting entity prior to the establishment of the business relationship.

(3) The reporting entity shall gather data referred in paragraph 1 of this Article through the examination of public or other available records, i.e. through the examination of documents and business documentation supplied by a bank or other credit institution seated in a third country.

(4) The reporting entity shall not be permitted to establish or to extend a correspondent relationship with a bank or other credit institution seated in a third country should:

1. the reporting entity fail to first gather data referred to in paragraph 1, items 1, 2, 4, 5 and 6 of this Article;
2. the employee fail to first obtain written consent from the superior responsible person of the reporting entity for the purposes of establishing a correspondent relationship;
3. the bank or other credit institution seated in a third country be without a money laundering and terrorist financing prevention and detection system in place or if the laws of the third country in which the said institutions shall be seated or registered shall not require the institutions to apply legal and other adequate regulations in the field of money laundering and terrorist financing prevention and detection;
4. the bank or other credit institution seated in a third country operate as a shell bank, i.e. if it establishes correspondent or other business relationships and conducts transactions with shell banks.

Foreign Politically Exposed Persons

Article 32

(1) The reporting entities shall be obliged to apply an adequate procedure to determine whether or not a customer is a foreign politically exposed person.

(2) The procedure referred to in paragraph 1 shall be defined through an internal reporting entity's enactment taking account of guidelines given by the competent supervisory body referred to in Article 83 of this Law.

(3) A foreign politically exposed person referred to in paragraph 1 of this Article shall be any natural person with permanent address or habitual residence in a foreign country who shall act or had acted during the previous year (or years) at a prominent public function, including their immediate family members, or persons known to be close associates of such persons.

(4) Natural persons who shall act or had acted at a prominent public function shall be:

a) presidents of countries, prime ministers, ministers and their deputies or assistants;
b) elected representatives of legislative bodies;
c) judges of supreme, constitutional and other high courts against whose verdicts, save for exceptional cases, legal remedies may not be applied;
d) judges of financial courts and members of central bank councils;
e) foreign ambassadors, consuls and high ranking officers of armed forces;
f) members of management and supervisory boards in government-owned or majority government-owned legal persons.

(5) The immediate family members referred to in paragraph 3 of this Article shall be: spouses or common-law partners, parents, siblings, as well as children and their spouses or common-law partners.

(6) The close associate referred to in paragraph 3 of this Article shall be any natural person who shall share common profits from property or an established business relationship, or a person with which the person referred to in paragraph 3 of this Article shall have any other close business contacts.

(7) Should the customer who shall establish a business relationship or conduct a transaction, i.e. should the customer on whose behalf the business relationship is being established or the transaction conducted be a foreign politically exposed person, the reporting entity shall in addition to the measures referred to in Article 8, paragraph 1 of this Law also take actions listed hereunder within the framework of the enhanced customer due diligence:

1. gather data on the source of funds and property which are or will be the subject matter of the business relationship or transaction, from documents and other documentation supplied by the customer. Should it be impossible to collect data in the described manner, the reporting entity shall collect data directly from a customer's written statement;
2. an employee of the reporting entity who shall run the procedure of business relationship establishment with a customer who is a foreign politically exposed person shall mandatorily obtain written consent from the superior responsible person before establishing such a relationship;
3. after the establishment of the business relationship, the reporting entity shall exercise due care in monitoring transactions and other business activities performed by a foreign politically exposed person with the reporting entity.

Customer's Absence during Identification and Identity Verification

Article 33

(1) If the customer was not physically present with the reporting entity during the identification and identity verification, in addition to the measures referred to in Article 8, paragraph 1 of this Law, the reporting entity shall be obliged to conduct one or more additional measures referred to in paragraph 2 of this Article within the framework of the enhanced customer due diligence.

(2) At customer identification and identity verification as referred to in paragraph 1 of this Article, the reporting entity shall be obliged to apply the following supplementary enhanced due diligence measures:

1. collect additional documents, data or information on the basis of which the customer's identity shall be verified;
2. additionally verify the submitted documents or additionally certify them by a foreign credit or financial institution referred to in Article 3, items 12 and 13 of this Law;
3. apply a measure whereby the first payment within the business activity is carried out through an account opened in the customer's name with the given credit institution.

(3) The establishment of a business relationship without physical presence of the customer shall not be permitted, unless the reporting entity shall apply the measure set forth in paragraph 2, item 3 of this Article.

New technologies

Article 34

(1) Credit and financial institutions shall be obliged to pay a special attention to any money laundering and/or terrorist financing risk which may stem from new technologies enabling anonymity (Internet banking, ATM use, tele-banking, etc.) and put policies in place and take measures aimed at preventing the use of new technologies for the money laundering and/or terrorist financing purposes.

(2) Credit and financial institutions shall be obliged to have policies and procedures in place for risks attached with a business relationship or transactions with non face to face customers and to apply them at the establishment of a business relationship with a customer and during the course of conducting customer due diligence measures, respecting the measures set forth in Article 33 of this Law

Sub-section 2

SIMPLIFIED CUSTOMER DUE DILIGENCE

General Provisions

Article 35

(1) By way of derogation from the provisions contained in Article 8, paragraph 1 of this Law, the reporting entities may at establishing the business relationship and at conducting transactions referred to in Article 9, paragraph 1, items 1 and 2 of this Law, except in instances when there are reasons for suspicion of money laundering or terrorist financing in relation to a customer or a transaction, conduct a simplified customer due diligence, if the customer is:

1. reporting entity referred to in Article 4, paragraph 2, items 1, 2, 3, 6, 7, 8, 9 and 10 of this Law or other equivalent institutions under the condition that such an institution shall be seated in a member-state or a third country;
2. state bodies, local and regional self-government bodies, public agencies, public funds, public institutes or chambers;
3. companies whose securities have been accepted and traded on the stock exchanges or the regulated public market in one or several member-states in line with the provisions in force in the European Union, i.e. companies seated in a third country whose securities have been accepted and traded on the stock exchanges or the regulated public market in a member-country or a third country, under the condition that the third country have the disclosure requirements in effect in line with the legal regulations in the European Union;
4. persons referred to in Article 7, paragraph 5 of this Law for which a negligent money laundering or terrorist financing risk shall exist.

(2) By way of derogation from the provisions contained in paragraph 1 of this Article, a reporting entity establishing a correspondent relationship with a bank or other credit institution seated in a third country shall conduct the enhanced customer due diligence in keeping with the provisions contained in Article 30, paragraph 1, item 1 of this Law.

Gathering and Verifying Customer Information

Article 36

(1) By way of derogation from the provisions contained in Article 8, paragraph 1 of this Law, the simplified customer due diligence referred to in Article 35 paragraph 1 of this Law shall encompass gathering and verifying certain data on the customer, business relationship and transaction.

(2) Within the framework of the simplified customer due diligence, the reporting entities shall be obliged to gather the following data:

1. at establishing a business relationship referred to in Article 9, paragraph 1, item 1 of this Law:
   - name, address, seat and business registration number of the legal person establishing the business relationship, i.e. the legal person on whose behalf the business relationship is being established;
   - name and surname of the legal representative or a person authorised by power of attorney who establishes business relationship on behalf of the legal person;
   - purpose and intended nature of the business relationship and date of the relationship establishment;
2. at conducting transactions referred to in Article 9, paragraph 1, item 2 of this Law:
   - name, address, seat and business registration number of the legal person for whom a transaction is being conducted;
   - name and surname of the legal representative or a person authorised by power of attorney who conducts the transaction on behalf of the legal person;
   - date and time of transaction execution;
   - transaction amount and currency in which the transaction is being executed;
   - manner of transaction execution;
   - purpose of the transaction;
   - name and seat of a legal person to whom the transaction is intended.

(3) The reporting entity shall gather information referred to in paragraph 2 of this Article through examination of original or notarised photocopies of excerpts from a court of other public register supplied to the reporting entity by the customer, i.e. through a direct examination of a court or other public register

(4) Should the manner described in paragraph 3 of this Article be insufficient to enable the collection of all required data, the reporting entity shall gather the missing data from the documents and other business documentation submitted or supplied by the customer to the reporting entity. If for objective reasons the missing data cannot be obtained in such a manner either, the reporting entity shall gather data on the basis of a written statement given by the customer's legal representative.

(5) Documentation referred to in paragraphs 3 and 4 of this Article must not be more than three months old at the submission to the reporting entity.

Section 6

LIMITATIONS IN DOING BUSINESS WITH CUSTOMERS

Prohibition of the Use of Anonymous Products

Article 37

The reporting entities shall not be allowed to open, issue or keep anonymous accounts, coded or bearer passbooks for customers, i.e. other anonymous products which would indirectly or directly enable the concealment of customer's identity.

Prohibition of Doing Business with Shell Banks

Article 38

The reporting entities shall be prohibited from establishing or continuing correspondent relationships with a bank which operate or could operate as a shell bank or with other similar credit institutions known to enter into agreements on opening and keeping accounts with shell banks.

Restrictions in Cash Operations

Article 39

(1) In the Republic of Croatia, cash collections exceeding the amount of HRK 105,000.00 or in the arrangements with non-residents valued in excess of EUR 15,000.00, shall not be permitted at:

- selling goods and rendering services;
- sales of real-estate;
- receiving loans;
- selling negotiable securities or stakes.

(2) The limitation of receiving cash payments referred to in paragraph 1 of this Article shall also be in effect in instances when the payment with the said transaction shall be conducted in several interrelated cash transactions jointly exceeding HRK 105,000.00, i.e. a value of EUR 15,000.00.

(3) The cash collection limitation shall pertain to all legal and natural persons who shall receive cash through the said transactions during the performance of their registered business activities.

(4) The collections exceeding the amounts prescribed in paragraphs 1 and 2 of this Article must be conducted via non-cash means through a bank account, unless provided for otherwise in another law.

Section 7

REPORTING TRANSACTIONS TO THE OFFICE

Cash Transactions Reporting Requirement and Deadlines

Article 40

(1) The reporting entities shall be obliged to report the Office on each transaction being conducted in cash totalling HRK 200,000.00 and more immediately, and no lather than within three days upon the execution of the transaction.

(2) When reporting the Office on a cash transaction, the reporting entities shall undertake to supply data referred to in Article 16, paragraph 1, items 1, 3, 5, 6 and 9 of this Law in the manner to be prescribed by the Minister of Finance in a rulebook.

(3) The Minister of Finance may issue a rulebook to also prescribe additional data the reporting entity shall undertake to obtain for the purpose of reporting the Office on cash transactions.

(4) The Minister of Finance may issue a rulebook to prescribe the conditions under which the reporting entities for certain customers shall not be obliged to supply the Office with data on cash transactions referred to in paragraph 1 of this Article.

Obligation concerning the production of a list of indicators for the detection of suspicious transactions and customers in relation to which reasons for suspicion of money laundering or terrorist financing shall exist

Article 41

(1) The reporting entities referred to in Article 4, paragraph 2 of this Law shall be obliged to produce a list of indicators for the detection of suspicious transactions and customers in relation with which reasons for suspicion of money laundering or terrorist financing shall exist.

(2) During the course of production of the list of indicators referred to in the previous paragraph of this Article, the reporting entities shall first of all take account of the specific features to their respective operations and the characteristics of a suspicious transaction referred to in Article 42, paragraph 7 of this Law.

(3) During the course of determining the reasons for suspicion of money laundering or terrorist financing and other circumstances thereof, the reporting entities shall be obliged to use the list of indicators referred to in paragraph 1 of this Article as basic guidelines for determining the reasons for suspicion of money laundering and terrorist financing.

(4) The list of indicators referred to in paragraph 1 of this Article shall be an integral part of the reporting entity's internal enactments, and the reporting entities shall be obliged to upgrade and adapt the list in accordance with the money laundering trends and typologies known to them, as well as with circumstances stemming from the operations of the given reporting entity.

(5) The Office, the Financial Inspectorate, the Tax Administration, the Croatian National Bank, the Croatian Financial Services Supervision Agency, the Croatian Chamber of Notaries Public, the Croatian Bar Association, the Croatian Tax Advisors Chamber, and associations and societies whose members shall be obliged to observe this Law shall cooperate with the reporting entities for the purpose of producing the list of indicators referred to in paragraph 1 of this Article.

(6) The Minister of Finance may issue a special rulebook to prescribe mandatory inclusion of individual indicators into the list of indicators for the detection of suspicious transactions and customers in relation to which reasons for suspicion of money laundering or terrorist financing shall exist.

Requirement and Deadlines for Reporting on Suspicious Transactions and Persons

Article 42

(1) The reporting entities shall be obliged to refrain from the conducting of a transaction for which the reporting entity shall know or suspect to be connected with money laundering, i.e. terrorist financing. The reporting entity shall be obliged to notify the Office on such a transaction without any undue delay before the transaction execution, and to indicate in the report the reasons for suspicion of money laundering or terrorist financing, as well as the deadline within which the transaction is to be conducted.

(2) The reporting entity shall be obliged to notify the Office of the intention or plan to conduct the suspicious transaction referred to in paragraph 1 of this Article notwithstanding of whether or not the transaction was subsequently conducted.

(3) Exceptionally, if the reporting entity was not in position to notify the Office of the suspicious transaction before its execution in instances referred to in paragraphs 1 and 2 of this Article due to the nature of the transaction or due to the fact that the transaction was not executed or for other justified reasons, the reporting entity shall be obliged to report the Office subsequently, and no later than the next business day. The suspicious transaction report is to substantiate the reasons for which the reporting entity was objectively unable to comply with what was prescribed.

(4) The reporting entities must supply the Office with the suspicious transaction reports containing data as referred to in Article 16, paragraph 1 of this Law by phone, fax or in other adequate manner before the conducting of a transaction, and after the conducting of transaction in the manner to be prescribed by the Minister of Finance in a rulebook. Should reporting entities fail to supply a written suspicious transaction report, they shall do so subsequently, and no later than next business day. The reporting entity and the Office are to produce a note on a report which was not supplied in writing.

(5) In the report referred to in the previous paragraph of this Article, the reporting entities shall undertake to indicate and substantiate the reasons referred to in paragraph 7, items 1, 2, 3 and 4 of this Article which shall point to the existence of reasons for suspicion of money laundering or terrorist financing in relation with a transaction or a customer.

(6) The Minister of Finance may issue a rulebook to prescribe additional data the reporting entity shall undertake to supply for the purpose of reporting the Office on suspicious transactions.

(7) The suspicious transaction referred to in paragraphs 1 and 2 of this Article shall be any attempted or conducted cash and non-cash transaction, irrespective of the value and the execution manner, if the reporting entity shall know, suspect or have grounds to suspect that:

1. the transaction involves funds stemming from illegal activities or is linked with terrorist financing given the ownership, nature, source, location or control of such funds;
2. the transaction by its properties associated with the status or other characteristics of customers or funds or other properties shall clearly diverge from the usual transactions of the same customer and which shall match the necessary number and type of indicators pointing to the existence of reasons for suspicion of money laundering and terrorist financing;
3. the transaction is intended to avoid regulations providing for money laundering or terrorist financing prevention measures;
4. in all instances when the reporting entity judges that there shall be reasons for suspicion of money laundering and terrorist financing in relation with a transaction or a customer.

Complex and Unusual Transactions

Article 43

(1) The reporting entities shall be obliged to pay a special attention to all complex and unusually large transaction, as well as to each unusual form of transactions without an apparent economic or visible lawful purpose even in instances when reasons for suspicion of money laundering or terrorist financing have not yet been detected in relation to such transactions.

(2) Concerning the transactions referred to in paragraph 1 of this Article, the reporting entities shall be obliged to analyse the background and purpose of such transactions, and to make a written record of the analysis results to be available at the request of the Office and other supervisory bodies referred to in Article 83 of this Law.

(3) By way of derogation from the provisions contained in paragraphs 1 and 2 of this Article, should the reporting entities detect suspicion of money laundering or terrorist financing they shall be obliged to observe the provisions of Article 42of this Law.

Section 8

AUTHORISED PERSON, TRAINING AND INTERNAL AUDIT

Authorised Person and his/her Deputy

Article 44

(1) The authorised person and his/her deputy shall be persons appointed by the reporting entity responsible for carrying out measures and actions undertaken for the purpose of money laundering and terrorist financing prevention and detection as prescribed by this law and regulations passed on the basis of this Law.

(2) The reporting entities referred to in Article 4, paragraph 2, items 1-15 of this Law shall be obliged to appoint one authorised person and one or more authorised person's deputies, and to inform the Office thereof immediately and no later than within 7 days after the appointment, i.e. change of data on the authorised person.

(3) Should the reporting entity referred to in Article 4, paragraph 2 of this Law fail to appoint an authorised person, the reporting entity's legal representative or other person in charge or running the arrangements of the reporting entity, i.e. the reporting entity's compliance officer as per legal regulations shall be deemed the authorised person.

Requirements for the Authorised Person and the Deputy

Article 45

(1) The reporting entity referred to in Article 4, paragraph 2, items 1-15 of this Law must ensure that the matters falling under the remit of the authorised person and the authorised person's deputy referred to in Article 44 of this Law be performed solely by persons who shall meet the following requirements:

- the person shall be employed at a position which was systematised within the organisational structure at such a level to enable the person execute the tasks prescribed by this Law and regulations passed on the basis of this Law in a quick, quality and timely fashion, as well as the independence in his/her work and direct communication with management;
- the person shall not be under a criminal proceeding, i.e. the person was not sentenced for an offence against the values protected by the international law, safety of payment operations and arrangements, credibility of documents, against property and the official duty for the period of 5 years upon the effectiveness of the sentence imposed on the person, with that the servitude time shall not be included in the said period;
- the person shall be adequately professionally trained to carry out tasks in the field of money laundering and terrorist financing prevention and detection and shall possess the capabilities and experience necessary for the performance of the authorised person's function; - the person is well familiar with the nature of reporting entities' operations in the fields exposed to money laundering or terrorist financing risk.

Duties of the Authorised Person and the Deputy

Article 46

(1) The authorised person and the deputy referred to in Article 44 of this Law shall be authorised to carry out all measures and actions prescribed in this Law, notably as follows:

1. catering for the establishment, operation and the development of the money laundering and terrorist financing prevention and detection system within the reporting entity;
2. catering for a regular and timely provision of data to the Office in keeping with this Law and the regulations passed on the basis of this Law;
3. partaking in the design of operational procedures and amendments thereof and in the production of reporting entity's internal enactments applicable to money laundering and terrorist financing prevention and detection;
4. partaking in the production of guidelines for carrying out internal audits relative to money laundering and terrorist financing prevention and detection;
5. monitoring and coordinating the activities of the reporting entity in the field of money laundering and terrorist financing prevention and detection;
6. partaking in the establishment and development of IT support for carrying out activities in the field of money laundering and terrorist financing prevention and detection with the reporting entity;
7. encouraging management board or other managerial body of the reporting entity and making suggestions for improving the money laundering and terrorist financing prevention and detection system with the reporting entity;
8. partaking in producing the professional improvement and training programme for employees of the reporting entity in the field of money laundering and terrorist financing prevention and detection.

(2) The authorised person's deputy shall replace the authorised person during his/her absence in the performance of matters referred to in paragraph 1 of this Article and shall perform other tasks as per this Law, should this be provided for by the reporting entity's internal enactment.

Duties of the Reporting Entity towards the Authorised Person and the Deputy

Article 47

(1) Within the framework of money laundering and terrorist financing prevention and detection as prescribed by this Law, the reporting entity shall be obliged to ensure the following conditions to the authorised person and the deputy:

1. unrestricted access to all data, information and documentation necessary for the purposes of money laundering and terrorist financing prevention and detection;
2. adequate authorisations for an efficient conducting of tasks referred to in Article 46, paragraph 1 of this Law;
3. adequate human resource, material and other work conditions;
4. adequate premises and technical conditions, which shall guarantee proper degree of confidential data and information protection available to the authorised person on the basis of this Law;
5. adequate IT support enabling ongoing and safe monitoring of the activities in the field of money laundering and terrorist financing prevention and detection;
6. regular professional training in relation to money laundering and terrorist financing prevention and detection;
7. replacement of the authorised person during absence.

(2) Internal organisational units, including management board or other managerial body within the reporting entity shall be obliged to ensure the authorised person and deputy have assistance and support during the performance of assignments as per this Law and regulations passed on the basis of this Law and to inform them of all the activities which were or might be related with money laundering or terrorist financing. The manner of referring the notifications and the course of

cooperation between the authorised person and the employees in other organisational units shall be provided for in detail in the reporting entity's internal enactments.

(3) The reporting entity shall be obliged to ensure the persons who perform the function of the authorised person and the deputy as per this Law carry out their work and assignments as an exclusive full time work duty, if the scope of tasks in the money laundering and terrorist financing prevention and detection field is permanently expanded due to the large number of employees, the nature or scope of operations, i.e. for other justified reasons.

(4) The authorised person referred to in paragraph 3 of this Article shall perform his/her duties as autonomous organisational section directly responsible to management board or other managerial body, and shall functionally and organisationally be segregated from other organisational parts of the reporting entity.

Reporting Entity's Internal Enactment

Article 48

(1) The reporting entities shall undertake to pass an internal enactment to provide for measures, actions and proceeding for the purpose of money laundering and terrorist financing prevention and detection as prescribed by this Law and regulations passed on the basis of this Law.

(2) The reporting entity's internal enactment is to specifically determine the responsibility of the authorised persons in charge of the implementation of this Law in the case of the non-observance of the provisions of this Law and regulations passed on the basis of this Law, as well as the responsibility of all other reporting entity's employees partaking in the implementation of this Law and regulations passed on the basis of this Law.

(3) The reporting entity shall be obliged to supply the Office with a copy of the internal enactment at Office's request.

Regular Professional Training and Development Obligation

Article 49

(1) The reporting entities referred to in Article 4, paragraph 2 of this Law shall be obliged to cater for regular professional improvement and training of all employees involved in the tasks relative to money laundering and terrorist financing prevention and detection as per this Law.

(2) Professional improvement and training referred to in paragraph 1 of this Article shall pertain to the familiarisation with the provisions of this Law and regulations passed on the basis of the Law, reporting entity's internal enactments, and with international standards stemming from the international money laundering and terrorist financing prevention conventions, with the guidelines and the list of suspicious transactions detection indicators, and with other assignments prescribed by this Law.

(3) No later than before the expiration of the current year, the reporting entity shall undertake to produce the annual professional improvement and training programme pertinent to the money laundering and terrorist financing prevention and detection field for the next calendar year.

Regular Internal Audit Obligation

Article 50

(1) The reporting entities referred to in Article 4, paragraph 2, items 1-15 of this Law shall be obliged to ensure that regular internal audit over the performance of money laundering and terrorist financing prevention and detection assignments as per this Law be performed at least once a year, and to inform the Office accordingly at request.

(2) The purpose of internal audit referred to in paragraph 1 of this Article shall relate to the detection and prevention of irregularities in the implementation of the Law and to the improvement of the internal system for detecting suspicious transactions and persons, as referred to in Article 42 of this Law.

(3) The Minister of Finance may issue a rulebook to prescribe more detailed internal auditing rules.

CHAPTER III

DUTIES OF LAWYERS, LAW FIRMS AND NOTARIES PUBLIC, AND AUDITING FIRMS AND INDEPENDENT AUDITORS, LEGAL AND NATURAL PERSONS INVOLVED IN THE PERFORMANCE OF ACCOUNTING SERVICES AND TAX ADVISORY SERVICES

General Provisions

Article 51

During the performance of matters from their respective scopes of competence as defined in other laws, lawyers, law firms and notaries public, and auditing firms and independent auditors, legal and natural persons involved in the performance of accounting services and tax advisory services (hereinafter referred to as the persons performing professional activities) shall be obliged to carry out money laundering and terrorist financing prevention and detection measures and to observe the provisions of this Law providing for duties and obligations of other reporting entities, unless set forth otherwise in this Chapter.

Tasks and Duties of Lawyers, Law Firms and Notaries Public

Article 52

By way of derogation from the provisions contained in Article 51 of this Law, lawyers, law firms or notaries public shall observe the provisions of this Law only in instances when:

1. assisting in planning or conducting transactions on behalf of a customer in relation with:
   a) buying or selling real-estate or stakes, i.e. shares in a company;
   b) management of cash funds, financial instruments or other customer-owned property;
   c) opening or managing bank accounts, savings deposits or financial instruments trading accounts;
   d) collecting funds necessary for the establishment, operation or management of a company;
   e) establishment, operation or management of an institution, a fund, a company or another legally defined organisational form;
2. carrying out real-estate related financial transaction or transactions on behalf and for the account of a customer.

Customer Due Diligence Conducted by Persons Involved in the Performance of Professional Activities

Article 53

(1) Within the framework of customer due diligence at establishing the business relationship referred to in Article 9, paragraph 1, item 1 of this Law, the persons involved in the performance of professional activities shall gather information referred to in Article 16, paragraph 1, items 1, 4, 5, 7, 8 and 10 of this Law.

(2) Within the framework of customer due diligence at conducting transactions referred to in Article 9, paragraph 1, item 2 of this Law, the persons involved in the performance of professional activities shall gather information referred to in Article 16, paragraph 1, items 1, 3, 4, 5, 6, 9 and 10 of this Law.

(3) Within the framework of customer due diligence in instances when there shall be suspicion of credibility and veracity of the previously collected customer or beneficial owner information, and in all instances when there shall be reasons for suspicion of money laundering or terrorist financing as referred to in Article 9, paragraph 1, items 3 and 4 of this Law, the persons involved in the performance of professional activities shall gather information referred to in Article 16, paragraph 1, items 1, 3, 4, 5, 6, 7, 8, 9, 10 and 11 of this Law.

(4) Within the framework of customer identification, the persons involved in the performance of professional activities shall identify the customer, i.e. customer's legal representative or the person authorised by power of attorney and shall gather information referred to in Article 16, paragraph 1, item 1 of this Law, through the examination of a customer's official personal identification document, i.e. original documents or notarised photocopies of documents or notarised documentation from a court or other public register, which may not be more than three months old.

(5) The persons involved in the performance of professional activities shall identify the beneficial owner of the customer, which beneficial owner shall be a legal person or another similar legal entity through the gathering of information referred to in Article 16, paragraph 1, item 4 of this Law, through examination or original or notarised photocopy of documentation from a court or other public register, which may not be more than three months old. Should the excerpts from a court or other public register be insufficient to enable the collection of all information, the missing information shall be collected through the examination of original or notarised photocopies of documents and other business documentation presented by the legal person's legal representative, i.e. his/her person authorised by power of attorney.

(6) The persons involved in the performance of professional activities shall gather other information referred to in Article 16, paragraph 1 of this Law through the examination of original or notarised photocopy of documents and other business documentation.

(7) Should it be impossible to obtain all data in the manner set forth in this Article, the missing information, except for information referred to in Article 16, paragraph 1, item 1, sub-item 5, item 5, sub-item 5 and item 11 of this Law, shall be gathered directly from a written statement given by the customer or customer's legal representative.

(8) At establishing a business relationship with a customer subject to the mandatory audit of annual accounting statements as prescribed by a law providing for the customer's business activity, an auditing firm and an independent auditor may conduct a simplified customer due diligence, save for instances where reasons for suspicion of money laundering or terrorist financing shall exist associated with a customer or circumstances of an audit.

(9) The persons involved in the performance of professional activities shall conduct customer due diligence measures referred to in paragraphs 1-7 of this Article to the extent and within the scope relevant to their scope of work.

Obligation of the persons involved in the performance of professional activities to report the Office on transactions and persons in relation to which reasons for suspicion of money laundering and terrorist financing shall exist

Article 54

(1) Should a lawyer, a law firm and a notary public, during the performance of matters referred to in Article 52 of this Law, as well as an auditing firm and an independent auditor, legal and natural persons involved in the performance of accounting services and tax advisory services, establish that reasons for suspicion of money laundering or terrorist financing shall exist in relation with a transaction or certain person, they shall undertake to notify the Office thereof without any undue delay pursuant to with the provisions contained in Article 42 of this Law.

(2) In all instances when the customer seeks an advice from persons involved in the performance of professional activities on money laundering or terrorist financing, the persons involved in the performance of professional activities shall undertake to immediately notify the Office thereof, and no later than within three business days from the date the customer sought for such an advice.

(3) At reporting the Office on suspicious transactions, the persons involved in the performance of professional activities shall furnish the Office with information referred to in Article 16, paragraph 1 of this Law in the manner to be prescribed by the Minister of Finance in a rulebook.

Exceptions for persons involved in the performance of professional activities

Article 55

(1) The provisions contained in Article 54, paragraphs 1 of this Law shall not apply to the persons involved in the performance of professional activities in respect of information they receive from or obtain on a customer during the course of establishing the legal position of the customer or during the representation of the customer in relation with a court proceeding which shall include advice on proposing or avoiding court proceeding, whether such information is received or obtained before, during or after the completion of such court proceedings.

(2) In the instance covered in paragraph 1 of this Article, the persons involved in the performance of professional activities shall not be obliged to supply data, information and documentation on the basis of the Office's request referred to in Article 59 of this Law. In such instances, they shall undertake to proceed without any undue delay and no later than within fifteen days from the receipt of the request supply the Office with a substantiated written explanation of reasons for which they did not comply with the Office's request.

(3) By way of derogation from the obligations prescribed in this Law, the persons involved in the performance of professional activities shall not be obliged:

1. to report the Office on cash transactions referred to in Article 40, paragraph 1 of this Law, except in instances when reasons for suspicion of money laundering or terrorist financing shall exist in relation with a transaction or a customer;
2. to appoint authorised persons and authorised person's deputy;
3. to carry out internal audit over the performance of money laundering and terrorist financing related tasks.

CHAPTER IV

TASKS AND SCOPE OF COMPETENCE OF THE ANTI-MONEY LAUNDERING OFFICE

General Provisions

Article 56

(1) The Office shall be an administrative organisation within the structure of the Ministry of Finance, performing tasks aimed at money laundering and terrorist financing prevention, as well as other tasks as provided for in this Law.

(2) As a Financial Intelligence Unit and the Central National Unit, the Office shall collect, store, analyse and submit data, information and documentation on suspicious transactions to competent government bodies for further proceeding for the purpose of money laundering and terrorist financing prevention and detection in keeping with the provisions contained in this Law.

(3) The Ministry of Finance shall submit the Office Performance Report at least once a year to the Government of the Republic of Croatia.

Money Laundering and Terrorist Financing Prevention

Article 57

(1) The Office shall be competent to perform the activities listed hereunder for the purpose of money laundering and terrorist financing prevention:

1. Acquiring and analysing information, data and documentation supplied by the reporting entities and other competent bodies in relation to money laundering and terrorist financing, issuing orders to reporting entities on temporary suspension of a suspicious transaction execution;
2. Requiring the reporting entities exercise ongoing monitoring of financial operations of customers;
3. Requiring data or other documentation necessary for money laundering and terrorist financing detection purposes from all government bodies, local and regional self-government units and legal persons with public authorities;
4. Effect inter-institutional cooperation in the field of money laundering and terrorist financing prevention and detection with all competent government bodies;
5. Reporting information to competent government bodies and foreign financial intelligence units in instances when reasons for suspicion of money laundering and terrorist financing shall exist in relation with a transaction or a person in the country or abroad;
6. Exchange of data, information and documentation with foreign financial intelligence units and other international bodies competent for money laundering and terrorist financing prevention matters;
7. Conducting offsite supervision via the collection and examination of data and documentation;
8. Obtaining and examining data and documentation necessary to carry out misdemeanour proceedings, and filing indictment motions;
9. Proposing to the a competent supervisory body the conducting of targeted onsite supervisions concerning the implementation of money laundering and terrorist financing prevention measures;

(2) In addition to the tasks referred to in paragraph 1 of this Article, the Office shall also perform the tasks indicated hereunder of relevance for the development of the preventive money laundering and terrorist financing prevention system, including:

1. Giving proposals to a competent body concerning amendments to regulations applicable to money laundering and terrorist financing prevention and detection;
2. Cooperating jointly with the supervisory bodies with the reporting entities during the production of the list of indicators for the detection of transactions and customers in relation to which reasons for suspicion of money laundering or terrorist financing shall exist;
3. Jointly with the regulatory bodies and supervisory bodies referred to in Article 83 of this Law, issuing guidelines for a uniform implementation of this Law and regulations passed on the basis of this Law, for reporting entities referred to in Article 4, paragraph 2 of this Law;
4. Taking part in professional training of employees from the reporting entities, government bodies and legal persons with public authorities;
5. Publishing statistical data relative to money laundering and terrorist financing at least once a year;
6. Informs the public in other adequate ways on the forms of money laundering and terrorist financing.

Inter-Institutional Cooperation of the Office

Article 58

(1) In the money laundering and terrorist financing prevention and detection, the Office shall cooperate with the State Attorney's Office of the Republic of Croatia, the Ministry of the Interior – the Police Directorate, the supervisory services of the Ministry of Finance (the Financial Inspectorate, the Customs Administration, the Tax Administration and the Financial Police), the Croatian Financial Services Supervision Agency, the Croatian National Bank, the Security-Intelligence Agency, the

Ministry of Foreign Affairs and European Integration, the Ministry of Justice and with other state bodies.

(2) For the purpose of achieving the strategic and operational objectives, the bodies referred to in paragraph 1 of this Article shall sign a protocol on cooperation and on the establishment of an inter-institutional money laundering and terrorist financing working group.

(3) The Office must have timely access, direct or indirect, to financial, administrative and security data, information and documentation relative to the implementation of this Law and regulations passed on the basis of this Law for the purpose of the Office's tasks performance, including the suspicious transactions analyses.

Section 1

ANALYTICAL-INTELLIGENCE WORK OF THE OFFICE: MONEY LAUNDERING AND TERRORIST FINANCING DETECTION

Sub-section 1

GENERAL PROVISIONS

Request for Reporting Entities' Supply of Suspicious Transactions or Persons Data

Article 59

(1) The Office shall commence the analytical processing of transactions in instances when a reporting entity or a competent body referred to in Articles 58 and 64 of this Law supplies the Office with substantiated reasons for suspicion of money laundering or terrorist financing in relation with a transaction or a person.

(2) The Office may order the reporting entities to supply all data required for money laundering and terrorist financing prevention and detection in instances when suspicion of money laundering or terrorist financing shall exist, when the Office had received:

1. a cash or suspicious transaction report from a reporting entity;
2. a written request or a suspicious transaction report or a notification on suspicion of money laundering or terrorist financing from a foreign financial intelligence unit;
3. a written report on suspicion of money laundering and terrorist financing from a body referred to in Article 58, paragraph 1 of this Law;
4. a written report referred to in Article 83, paragraph 1, items b) to e) of this Law.

(3) The Office may require the reporting entities referred to in Article 4, paragraph 2 of this Law supply the Office with other data necessary for the money laundering and terrorist financing prevention and detection purposes, such as:

1. data on customers and transactions the reporting entities shall gather in keeping with the provisions contained in Article 16 of this Law;
2. data on the status of funds and other customer's property with the reporting entity;
3. data on the customer's funds and property turnover with the reporting entity;
4. data on other business relationships of the customers established with the reporting entity;
5. all other data and information the reporting entity had gathered or keep on the basis of this Law, which data and information shall be required for money laundering or terrorist financing prevention and detection purposes.

(4) The Office may require the reporting entities supply data referred to in paragraph 3 of this Article in instances involving a person which may be assumed to have taken part, i.e. is involved in any way whatsoever in the transactions or matters of a person in relation to which reasons for suspicion of money laundering or terrorist financing shall exist.

(5) In instances referred to in paragraphs 2, 3 and 4 of this Article, the reporting entities shall undertake to supply the Office with all accompanying documentation at request of the Office.

(6) The reporting entities must furnish the Office with data, information and documentation referred to in the previous paragraphs of this Article without any undue delay, and no later than within fifteen days after the request receipt date.

(7) The Office may set a shorter deadline in its request, should this be necessary for the purpose of determining circumstances of relevance for the issuance of a temporary suspicious transaction execution suspension order, or for referring data to a foreign financial intelligence unit, and in other necessary instances when such a course of action shall be required to prevent the causing of economic damage.

(8) Because of the comprehensiveness of documentation and for other justified reasons, the Office may at reporting entity's substantiated written request allow an extension of the deadline referred to in paragraphs 6 and 7 of this Article, which extension shall also be given in writing.

(9) In the case referred to in paragraph 8 of this Article, the Office shall be entitled to conduct examination and immediate review of documentation with the reporting entities referred to in Article 4, paragraph 2 of this Article.

Order to Reporting Entities on Temporary Suspension of a Suspicious Transaction Execution

Article 60

(1) Should it be necessary to take urgent action to verify data on a suspicious transaction or a person or when the Office shall judge that there are grounded reasons that a transaction or a person is linked with money laundering or terrorist financing, the Office may issue a written order to instruct the reporting entity to temporarily suspend the execution of the suspicious transaction for a maximum period of 72 hours.

(2) In instances where it shall not be possible to issue the written order to the reporting entities due to the nature or manner of transaction execution, i.e. the circumstances surrounding the transaction, as well as in other urgent instances, the Office may exceptionally give the reporting entity a verbal order to temporarily suspend the execution of the suspicious transaction.

(3) The Office must confirm the verbal order referred to in paragraph 2 of this Article by a written order immediately, and no later than within 24 hours after the verbal order had been issued.

(4) The reporting entity's authorised person shall make an official note on the receipt of the verbal order referred to in paragraph 2 of this Article, and keep the note on file in line with the provisions of this Law providing for the data protection and keeping.

(5) The Office shall without any undue delay notify the State Attorney's Office of the Republic of Croatia and/or the competent State Attorney's Branch of the issued orders referred to in paragraphs 1 and 2 of this Article.

(6) After the expiration of the deadline referred to in paragraph 1 of this Article, the transaction may be suspended only on the basis of a court decision in agreement with the provisions contained in a law providing for criminal procedure.

Cessation of the Temporary Suspicious Transaction Execution Suspension Order

Article 61

If within 72 hours from the issuance of the temporary suspicious transaction execution suspension order the Office had examined data on suspicious transaction and judged that grounded reasons for suspicion of money laundering and terrorist financing shall no longer exist, the Office shall inform the

State Attorney's Office of the Republic of Croatia and/or competent State Attorney's Branch and the reporting entity, who shall be allowed to immediately conduct the transaction.

Ordering Reporting Entities to Exercise Ongoing Monitoring of Customer's Financial Operations

Article 62

(1) The Office may give a reporting entity a written order to exercise ongoing monitoring of financial operations of a person in relation to which reasons for suspicion of money laundering or terrorist financing shall exist or of another person for which a grounded conclusion may be made that the person have assisted or taken part in the transactions or arrangements of a person in relation to which suspicion shall exist, and to regularly report the Office on transactions or arrangements the said persons shall perform or intend to perform with the reporting entity. The Office's order shall mandatorily define the deadlines within which the reporting entities shall be obliged to furnish the Office with the requested data.

(2) The reporting entities shall be obliged to furnish the Office with data referred to in paragraph 1 of this Article before the execution of a transaction or entering into an arrangement and to indicate the deadline in the report in which the transaction or the arrangement shall be completed.

(3) If the reporting entity shall not be in position to observe the provisions contained in paragraph 2 of this Article due to the nature of the transaction, i.e. the arrangement, or because of other justified reasons, the reporting entity shall undertake to furnish the Office with data at soonest occasion possible, and no later than on the next business day. The reporting entity's report must mandatorily indicate the reason for which the reporting entity failed to observe paragraph 2 of this Article.

(4) The implementation of the measures referred to in paragraph 1 of this Article may last for up to three months, and in the case of justified reasons the effectiveness of the measures may be prolonged each time for an additional month, with that the implementation of the measures may last for a maximum of six months.

Request to State Bodies, Local and Regional Self-Government Units, Legal Persons with Public Authorities for the Supply of Suspicious Transactions or Persons Information

Article 63

(1) Should the Office deem that reasons for suspicion of money laundering or terrorist financing shall exist in relation with a transaction or a person, the Office may request state bodies, local and regional self-government units, and legal persons with public authorities to supply data, information and documentation necessary for the money laundering or terrorist financing prevention and detection purposes.

(2) The Office also may request data referred to in paragraph 1 of this Article from state bodies, local and regional self-government units, and legal persons with public authorities in instances involving a person which may be assumed to have taken part, i.e. to have been involved in transactions or arrangements of a person in relation to which reasons for suspicion of money laundering or terrorist financing shall exist.

(3) State bodies, local and regional self-government units, and legal persons with public authorities shall be obliged to refer data, information and documentation from the previous paragraphs to the Office without any undue delay, and no later than within fifteen days upon the receipt of the request, or shall enable the Office to have free of charge direct electronic access to the specific data and information.

(4) By way of derogation from the provisions contained in paragraph 3 of this Article, the Office may exceptionally set a shorter deadline in its request, should such a course of action be necessary for

establishing circumstances of relevance for the issuance of a temporary suspicious transaction execution suspension order or for furnishing foreign financial intelligence units with necessary information, and in other necessary instances when such a course of action shall be required to prevent the causing of economic damage.

(5) Because of the comprehensiveness of documentation and for other justified reasons, the Office may at substantiated written request submitted by a state body, a local and regional self-government unit and a legal person with public authorities allow an extension of the deadline referred to in paragraphs 3 and 4 of this Article, which extension shall also be given in writing.

Reporting the Office by State Bodies, Courts, Legal Persons with Public Authorities and other Entities on Suspicion of Money Laundering and Terrorist Financing

Article 64

(1) By way of derogation from the provisions contained in Articles 40, 42 and 54, paragraphs 1 and 2 of this Law, the Office may commence analytical processing of suspicious transactions at a substantiated written proposal of the bodies referred to in Article 58, paragraph 1 of this Law, as well as of the courts and legal persons with public authorities, should the said proposals shall indicate reasons for suspicion of money laundering or terrorist financing and if such reasons were established during the performance of matters from the respective scopes of competence of the entities which filed such proposals.

(2) The Stock-Exchange, the Central Depositary Agency and the Croatian Privatisation Fund shall be obliged to notify the Office in writing and without any undue delay should they establish or detect such activities during the course of carrying out their respective matters, i.e. the arrangements they perform within the framework of their respective scopes of competence, which activities shall be or might be connected with money laundering or terrorist financing.

(3) The written proposal referred to in paragraphs 1 and 2 of this Article must contain reasons for suspicion of money laundering or terrorist financing with an explanation, including the following information:

1. name, surname, date and place of birth, permanent address of a natural person, i.e. name, address and seat of a legal person, in respect of which natural or legal persons reasons for suspicion of money laundering or terrorist financing shall exist or other identification information;
2. information on the transaction in respect of which reasons for suspicion of money laundering or terrorist financing shall exist (subject matter, amount, currency, date or period of transaction execution or other transaction-related information);
3. reasons for suspicion of money laundering or terrorist financing.

(4) Should the written proposal referred to in paragraphs 1 and 2 of this Article fall short of the explanation and information referred to in paragraph 3 of this Article, the Office shall refer the written proposal back to the body or person which submitted it for further completion.

(5) If the written proposal was not supplemented within 15 days or if the proposal again fails to substantiate the reasons and indicate information in keeping with the provisions contained in paragraph 3 of this Article, the Office shall notify the supplier of the proposal in writing as to the invalidity of the written proposal for the analytical processing purposes, indicating the reasons for which the proposal was not subject to analytical processing procedure.

(6) Exceptionally and if the circumstances surrounding the specific case allow so, the Office may commence the suspicious transactions analytical processing also on the basis of available data on persons and transactions referred to in paragraph 3, items 1 and 2 of this Article.

(7) At the request of the Office, the bodies referred to in paragraphs 1 and 2 of this Article shall be obliged to supply information, data and documentation pointing to the suspicion of money laundering or terrorist financing.

Report on Transactions Suspicious for Money Laundering and Terrorist Financing

Article 65

(1) In instances when the Office deems on the basis of analytical processing of data, information and documentation the Office had collected in line with this Law that reasons for suspicion of money laundering or terrorist financing in the country or abroad shall exist in relation with a transaction or a person, the Office shall accordingly and in writing report the competent state bodies or foreign financial intelligence units thereof, with that the report shall contain all necessary documentation.

(2) In the report referred to in paragraph 1 of this Article, the Office shall not state information on the reporting entity's employee who first supplied the information on the basis of Articles 42 and 54 of this Law, except for instances where reasons for suspicion shall exist that the reporting entity or its employee had committed the money laundering or terrorist financing offence, or if the information shall be necessary to establish the offence in the criminal procedure and the said information is required by the competent court in writing.

Feedback

Article 66

Concerning the received and analysed information regarding a transaction or a person for which reasons for suspicion of money laundering or terrorist financing were established, the Office shall supply a written notification thereof to the reporting entities referred to in Article 4, paragraph 2 of this Law who reported the transaction, save for instances in which the Office deems such a course of action could damage the further course and outcome of the proceeding, by doing the following:

1. confirm the transaction report receipt;
2. supply the information on the decision or the result of such a case if the case based on the report on transaction was closed or completed, and information thereof became available;
3. at least once a year, supply or publish statistical data on the received transaction reports and the results of proceedings;
4. supply or publish information on the current techniques, methods, trends and typologies of money laundering and terrorist financing;
5. supply or publish summarised examples of specific money laundering and terrorist financing cases.

Sub-section 2

INTERNATIONAL COOPERATION OF THE OFFICE

General Provisions

Article 67

(1) The provisions on international cooperation contained in this Law shall pertain to cooperation between the Office and the foreign financial intelligence units in respect of the exchange of relevant data, information and documentation at a request of the Office extended to a foreign financial intelligence unit, at request of a foreign financial intelligence unit extended to the Office and at own initiative (spontaneously) extended to a foreign financial intelligence unit, for the purpose of money laundering and terrorist financing prevention.

(2) Prior to the reference of personal information to foreign financial intelligence units, the Office may seek assurances that the country or the beneficiary being supplied with data have personal

information protection in place and that the foreign financial intelligence unit shall use personal information only for purposes provided for by this Law.

(3) The Office may sign memoranda of understanding with foreign financial intelligence units for the purpose of enhancing cooperation with regard to data, information and documentation exchange in the field of money laundering and terrorist financing prevention.

(4) By way of derogation from the provisions contained in this Article and in Articles 68, 69, 70 and 71 of this Law, the condition of effective reciprocity shall not be applied to international cooperation between the Office and foreign financial intelligence units and other foreign bodies and international organisations competent for money laundering and terrorist financing prevention from member-states.

Data Supply Requests Extended to Foreign Financial Intelligence Units

Article 68

(1) Within the framework of carrying out money laundering and terrorist financing prevention and detection tasks, the Office may extend requests to foreign financial intelligence units to supply the Office with data, information and documentation needed for money laundering or terrorist financing prevention and detection purposes.

(2) The Office shall be allowed to use data, information and documentation obtained on the basis of paragraph 1 of this Article solely for the needs of its analytical-intelligence work and for purposes provided for by this Law.

(3) Without a prior consent given by a foreign financial intelligence unit, the Office shall not be allowed to submit the received data, information and documentation to or present them for examination by a third person, natural or legal, i.e. to other body, or to use them for purposes contrary to the conditions and limitations set by the foreign financial intelligence unit to which the request was extended, and shall be obliged to apply the confidentiality classification to such data at least to the extent applied by the body which supplied such data.

Supply of Data at Request Extended by a Foreign Financial Intelligence Unit

Article 69

(1) The Office shall submit data, information and documentation on customers or transactions in respect of which reasons for suspicion of money laundering or terrorist financing shall exist, which the Office shall collect or keep in line with the provisions contained in this Law, to a foreign financial intelligence unit at such unit's request sent in writing on the basis of the effective reciprocity.

(2) The Office may refuse the satisfaction of the request of the foreign financial intelligence unit in the following cases:

1. if the Office deems on the basis of the facts and circumstances indicated in the request that the reasons for suspicion of money laundering or terrorist financing have not been supplied;
2. if the supply of data would jeopardize or could jeopardize the carrying out of a criminal procedure in the Republic of Croatia, i.e. if it could in any way damage the national interests of the Republic of Croatia.

(3) The Office shall notify the foreign financial intelligence unit that extended a written request of the refusal of the request referred to in paragraph 2 of this Article, stating the reasons for which the request extended by the foreign financial intelligence unit was not satisfied.

(4) The Office may set additional conditions and limitations under which the foreign financial intelligence unit shall be allowed to use data referred to in paragraph 1 of this Article.

Spontaneous Delivery of Information to a Foreign Financial Intelligence Unit

Article 70

(1) The Office shall be entitled to spontaneously deliver data and information, which the Office shall collect or keep in line with the provisions contained in this Law, concerning customers or transactions in relation to which reasons for suspicion of money laundering or terrorist financing shall exist to a foreign financial intelligence unit when the conditions of effective reciprocity shall be met.

(2) In terms of spontaneous delivery of data at Office's own initiative, the Office shall be entitled to set additional requirements and limitations under which the foreign financial intelligence unit shall be allowed to use the received data referred to in paragraph 1 of this Article.

Temporary Transaction Execution Suspension at the Proposal of a Foreign Financial Intelligence Unit

Article 71

(1) At a substantiated written proposal given by a foreign financial intelligence unit the Office may, under the conditions provided for by this Law and on the basis of the effective reciprocity, issue a written order to instruct a reporting entity to temporarily suspend a suspicious transaction execution for up to 72 hours.

(2) The Office shall notify the State Attorney's Office of the Republic of Croatia of the issued order referred to in paragraph 1 of this Article without any undue delay.

(3) The Office shall take such a course of action as prescribed in the provisions contained in paragraph 1 of this Article should it deem on the basis of reasons for suspicion indicated in the written proposal of the foreign financial intelligence unit that:

1. the transaction is connected with money laundering or terrorist financing and that
2. the transaction would have been temporarily suspended had the transaction been the subject matter of a domestic suspicious transaction report in keeping with the provisions contained in Articles 42 and 54 of this Law.

(4) The Office shall not consider a proposal of a foreign financial intelligence unit if the Office judges on the basis of the facts and circumstances stated in the proposal referred to in paragraph 1 of this Article that the reasons of money laundering or terrorist financing suspicion were not substantiated. The Office shall notify the foreign financial intelligence unit of the non-acceptance of the proposal, stating the reasons for which the proposal was not accepted.

(5) Concerning the order for a temporary transaction execution suspension as per this Article, the provisions contained in Articles 60 and 61 of this Law shall adequately apply.

Proposal to a Foreign Financial Intelligence Unit for a Temporary Transaction Execution Suspension Abroad

Article 72

Within the framework of carrying out money laundering and terrorist financing prevention and detection tasks, the Office may submit a written proposal to a foreign financial intelligence unit for a temporary suspension of transaction execution, should the Office judge that there shall exist reasons for suspicion of money laundering or terrorist financing associated with a person or a transaction.

Sub-section 3

DATA ACCESS AND INFORMATION EXCHANGE

Supplying Data to Courts and the competent State Attorney's Office

Article 73

At a substantiated written request filed by courts and the competent State Attorney's Office, the Office shall supply them with data on cash transactions referred to in Article 40, paragraph 1 and data on transactions referred to in Article 74 of this Law, which data shall be indispensable for them in establishing circumstances of relevance for confiscating economic benefits or determining provisional security measures in accordance with the provisions of a law providing for criminal proceeding.

Section 2

TASKS OF THE CUSTOMS ADMINISTRATION OF THE REPUBLIC OF CROATIA

Cash Carrying Across the State Border

Article 74

(1) The bodies of the Customs Administration of the Republic of Croatia shall be obliged to immediately notify the Office of any declaration of cash entering or leaving across the state border amounting to kuna equivalent of EUR 10,000.00 or more, and no later than within three days from the date of cash crossing the state border.

(2) The bodies of the Customs Administration of the Republic of Croatia shall be obliged to immediately notify the Office of any cash entering or leaving across the state border in instances when such cash carrying was not declared to a customs body, and no later than within three days from the date of cash crossing the state border.

(3) The bodies of the Customs Administration of the Republic of Croatia shall be obliged to notify the Office within a maximum of three days from the date of cash entering or leaving across the state border also in instances when such cash entering or leaving or attempted cash entering or leaving across the state border involves cash amounts less than kuna equivalent of EUR 10,000.00, should reasons be established for suspicion of money laundering or terrorist financing in relation with the person carrying cash, the manner of such cash carrying or other cash carrying circumstances.

(4) The Minister of Finance shall issue a rulebook to prescribe what shall be considered cash referred to in paragraph 1 of this Article and which data shall be supplied to the Office by the Customs Administration of the Republic of Croatia, as well as the manner of such data supply.

(5) From the date of Republic of Croatia’s accession to the European Union, the state border referred to in paragraphs 1, 2 and 3 of this Article shall be European Union border.

CHAPTER V

DATA PROTECTION AND KEEPING

Section 1

DATA PROTECTION

Secrecy of the Collected Data and of the Procedures

Article 75

(1) The reporting entities referred to in Article 4, paragraph 2 of this Law and their employees, including members of management and supervisory boards and other managerial bodies and other persons who have any type of access and availability of data collected in accordance of this Law shall not be allowed to disclose the information listed hereunder to a customer or a third person:

1. that the Office was or will be supplied with a piece of data, information or documentation on the customer or a third person or a transaction referred to in Article 42, Article 54, paragraphs 1 and 2 and Article 59 of this Law;
2. that the Office had temporarily suspended the execution of a suspicious transaction, i.e. gave instructions thereof to the reporting entity on the basis of Article 60 of this Law;
3. that the Office requested ongoing monitoring of a customer's financial operations on the basis of Article 62 of this Law;
4. that a pre-investigative procedure has commenced or might be commenced against a customer or a third person due to suspicion of money laundering or terrorist financing.

(2) The Office shall not be allowed to communicate the collected data, information and documentation and the course of action on the basis of this Law to persons to which data, information and documentation or action shall pertain, or to third persons.

(3) Information referred to in paragraphs 1 and 2 of this Article, reports on transactions suspected to be linked with money laundering or terrorist financing referred to in Article 65 of this Law shall be defined and marked as classified data and shall bear an adequate level of secrecy attributed to them.

(4) The Head of the Office, and the person authorised by the Head of the Office to that end shall be entitled to decide on data declassifying and the exclusion from data secrecy observance.

(5) The prohibition of information disclosure referred to in paragraph 1 of this Article shall not be valid if:

1. data, information and documentation collected and kept by the reporting entity in accordance with this Law shall be needed for the purpose of establishing facts in a criminal procedure and if the supply of such data was requested from or ordered to the reporting entity by a competent court in writing;
2. data from the previous item shall be required by a competent supervisory body referred to in Article 83 of this Law for the purpose of conducting supervision over a reporting entity in its implementation of the provisions of this Law and the initiation of a misdemeanour procedure.

(6) An attempt on the part of persons involved in the performance of professional activities referred to in Article 4, paragraph 2 to dissuade a customer from engaging in an illegal activity shall not represent information disclosure within the meaning of paragraph 1 of this Article.

Exemptions from the Data Secrecy Principle Observance

Article 76

(1) For the reporting entities referred to in Article 4, paragraph 2 of this Law, the state administration bodies, the legal persons with public authorities, the courts and the State Attorney's Office and their employees, the submission of data, information and documentation to the Office on the basis of this Law shall not represent the disclosure of classified data, i.e. disclosure of business, banking, professional, notary public, lawyer client privilege or other secret.

(2) The reporting entities referred to in Article 4, paragraph 2 of this Law and their employees shall not be held accountable for any damage caused to customers or third persons if they shall act bona fide in line with the provisions contained of this Law and regulations passed on the basis of this Law and:

1. supply the Office with data, information and documentation on their customers;
2. collect and process customer data, information and documentation;
3. carry out an order issued by the Office on temporary transaction suspension and instructions in relation with the order;
4. carry out an order issued by the Office on ongoing monitoring of customer's financial operations.

(3) The employees of the reporting entities referred to in Article 4, paragraph 2 of this Law may not be held disciplinary or criminally answerable for the infringement of classified data secrecy observance, i.e. data related to banking, professional, notary public, lawyer client privilege or other secret if:

1. they analyse data, information and documentation gathered in accordance with this Law for the purpose of establishing reasons for suspicion of money laundering or terrorist financing in relation to a customer or a transaction;
2. they supply the Office with data, information and documentation in keeping with the provisions contained in this Law or regulations passed on the basis of this Law.

Use of the Collected Data

Article 77

(1) The Office, the reporting entities referred to in Article 4, paragraph 2 of this Law, the state bodies, the legal persons with public authorities and other entities referred to in Article 64 of this Law and their employees shall be allowed to use data, information and documentation they gathered in accordance with this Law only for the money laundering and terrorist financing prevention and detection purposes, unless prescribed otherwise.

(2) The courts and the competent State Attorney's Offices shall be allowed to use data they received on the basis of Article 73 of this Law solely for the intended purpose of receipt.

Section 2

DATA KEEPING

Period of Data Keeping by the Reporting Entities

Article 78

(1) The reporting entities referred to in Article 4, paragraph 2, items 1-15 of this Law shall undertake to keep data collected on the basis of this Law and regulations passed on the basis of this Law and the accompanying documentation for the period of ten years after a transaction execution, the termination of a business relationship, entry of a customer into a casino or approaching a safe deposit box.

(2) The reporting entities referred to in Article 4, paragraph 2, items 1-15 of this Law shall undertake to keep data and the accompanying documentation on an authorised person and the authorised person's deputy, the professional training of employees and the performance of internal audit referred to in Articles 44, 49 and 50 of this Law for the period of four years after the appointment of the authorised person and the authorised person's deputy, the delivery of professional training or the performed internal audit.

(3) By way of derogation from the provisions contained in paragraph 1 of this Article, lawyers, law firms and notaries public, auditing firms and independent auditors, legal and natural persons involved in the performance of accounting services and tax advisory services shall undertake to keep data and the accompanying documentation they collected on the basis of Article 53 of this Law for the period of ten years after the completion of customer identification.

(4) By way of derogation from the provisions contained in paragraph 2 of this Article, lawyers, law firms and notaries public, auditing firms and independent auditors, legal and natural persons involved in the performance of accounting services and tax advisory services shall undertake to keep data and the accompanying documentation on professional training of employees for the period of four years after the delivery of professional training.

Period of Data Keeping by the Customs Administration of the Republic of Croatia

Article 79

The bodies of the Customs Administration of the Republic of Croatia shall undertake to keep data referred to in Article 74 of this Law for the period of twelve years from the collection date. Upon the expiration of the period, data and information shall be destroyed pursuant to the law providing for archives content and archives.

Data Keeping Period in the Office

Article 80

(1) The Office shall undertake to keep data and information from the records the Office shall keep in accordance with this Law for the period of twelve years from the collection date. Upon the expiration of the period, data and information shall be destroyed pursuant to the law providing for archives content and archives.

(2) Persons to which data and information shall pertain shall be entitled to have insight into personal data, i.e. to the transcription, excerpt or photocopy upon the expiration of the period of eleven years after the collection date.

Section 3

RECORDS AND STATISTICS KEEPING

Records Keeping

Article 81

(1) The reporting entities referred to in Article 4, paragraph 2, items 1-15 shall keep the following records:

1. records on customers, business relationships and transactions referred to in Article 9 of this Law;
2. records on the supplied data referred to in Articles 40 and 42 of this Law.

(2) Lawyers, law firms and notaries public, auditing firms and independent auditors, legal and natural persons involved in the performance of accounting services and tax advisory services shall keep the following records:

1. records on customers, business relationships and transactions referred to in Article 9 of this Law;
2. records on the supplied data referred to in Article 54, paragraph 1 and 2 of this Law.

(3) All reporting entities referred to in Article 4, paragraph 2 of this Law shall keep records on examinations conducted by supervisory bodies referred to in Article 83 of this Law of data, information and documentation referred to in Article 75, paragraph 1 of this Law, which records shall include data as follows:

1. name of the supervisory body;
2. name and surname of the authorised officer who conducted the examination;
3. date and time of data examination.

(4) The Customs Administration Bodies shall keep the following records:

1. records on the declared and undeclared cash entering and leaving in the domestic or foreign currency amounting to kuna equivalent of EUR 10,000.00 or more when crossing the state border;

2. records on cash entering or leaving or attempted cash entering or leaving in the domestic or foreign currency when crossing the state border in an amount below kuna equivalent of EUR 10,000.00 in relation to which there reasons for suspicion of money laundering or terrorist financing had existed.

(5) The Office shall keep the following records:

1. records on persons and transactions referred to in Articles 40 and 42 of this Law;
2. records on persons and transactions referred to in Article 54, paragraphs 1 and 2 of this Law;
3. records on the issued temporary suspicious transactions execution suspension orders referred to in Article 60 of this Law;
4. records on orders issued by the Office on conducting ongoing monitoring of customers financial operations referred to in Article 62 of this Law;
5. records on the received written proposals referred to in Article 64 of this Law;
6. records on the reports referred to in Article 65 of this Law;
7. records on international requests referred to in Articles 68, 69 and 70 of this Law;
8. records on temporary transaction execution suspensions at the proposal of foreign financial intelligence units referred to in Article 71 of this Law and on proposals given to foreign financial intelligence units on temporary transaction execution suspension abroad as referred to in Article 72 of this Law;
9. records on criminal and misdemeanour procedures referred to in Article 82 of this Law;
10. records on the measures taken as referred to in Article 86 and infringements referred to in Article 89 of this Law;
11. records on reporting the Office by competent supervisory bodies referred to in Article 87 of this Law concerning the suspicion of money laundering or terrorist financing.

(6) The contents of records referred to in paragraphs 1, 2 and 4 shall be prescribed by the Minister of Finance in a rulebook.

Statistics Keeping

Article 82

(1) For the purposes of making an assessment of the effectiveness of the overall system for combating money laundering and terrorist financing, the competent State Attorney's Office branches, the competent courts and competent state bodies shall undertake to keep comprehensive statistics and to supply the Office with data on proceedings being run on the account of money laundering and terrorist financing offences, as well as misdemeanour proceedings being run on the accounts of misdemeanours prescribed by this Law.

(2) The competent courts and the competent State Attorney's Office branches shall undertake to supply the Office twice a year with data on investigation initiation, legal effectiveness of indictments, effectiveness of verdicts for offence of concealment of the illegally obtained monies and terrorist financing, and on other predicate offences in relation with money laundering in the manner and within deadlines to be prescribed by the Minister of Finance in a rulebook.

(3) In the cases involving the completed first-instance misdemeanour proceeding on the account of misdemeanours prescribed by this Law, the Financial Inspectorate shall supply the Office with data in the manner and within deadlines to be prescribed by the Minister of Finance in a rulebook.

(4) Other competent state bodies shall undertake to notify the Office once a year, and no later than by end-January of the current year for the previous year, of the stages of proceedings and measures they took by way of the received suspicious transactions reports referred to in Article 65 of this Law.

CHAPTER VI

SUPERVISION OVER THE REPORTING ENTITIES

Section 1

GENERAL PROVISIONS

Supervisory Bodies and their Actions

Article 83

(1) The supervision of operations of the reporting entities referred to in Article 4, paragraph 2 of this Law concerning the application of this Law and regulations passed on the basis of this Law shall be conducted by the institutions listed hereunder within the framework of their respective scopes of competence:

a) the Office;
b) the Financial Inspectorate of the Republic of Croatia;
c) the Tax Administration;
d) the Croatian National Bank;
e) the Croatian Financial Services Supervision Agency.

(2) Should any of the supervisory bodies referred to in paragraph 1 of this Article establish during the conducting of supervision or in any other manner that grounds shall exist for suspicion that an offence prescribed in this Law was committed, they shall be obliged to file a motion to the Financial Inspectorate and take other measures and actions legally vested in them.

Section 2

SUPERVISORY BODIES' SCOPES OF COMPETENCE

The Office

Article 84

(1) The Office shall conduct offsite supervision of compliances with this Law with the reporting entities referred to in Article 4, paragraph 2 of this Law via the collection and examination of data, information and documentation supplied as per this Law.

(2) The reporting entities referred to in Article 4, paragraph 2 of this Law shall undertake to supply the Office with data, information and documentation prescribed by this Law, as well as other data the Office shall require for the conducting of supervision without any undue delay, and no later than within 15 days after the receipt of the request.

(3) The Office shall be entitled to require the state bodies, local and regional self-government units and legal persons with public authorities to supply the Office with all data, information and documentation it may require for the conducting of offsite supervision as per this Law and for the initiation of a misdemeanour proceeding.

(4) The Office may coordinate the work of other supervisory bodies and to require them to conduct targeted supervisions.

(5) The Office may sign Agreements of Understanding with other supervisory bodies.

Other Supervisory Bodies

Article 85

(1) The Financial Inspectorate shall conduct supervision of compliance with this Law with all reporting entities referred to in Article 4, paragraph 2 of this Law. The supervision of the reporting entities by the Financial Inspectorate shall be conducted on the basis of money laundering and

terrorist financing risk assessment. The Financial Inspectorate shall be entitled to use the assistance from other supervisory bodies in the conducting of supervision of the reporting entities in line with the signed agreements of understanding.

(2) The Tax Administration shall conduct supervision of compliance with this Law with the reporting entities referred to in Article 4 paragraph 2, item 13 of this Law. During the conducting of onsite supervision from its scope of competence, the Tax Administration shall also check whether or not domestic legal and natural persons comply with the prescribed limitation of cash payments in keeping with the provisions contained in Article 39 of this Law

(3) The Croatian National Bank shall conduct supervision of compliance with this Law with the reporting entities referred to in Article 4, paragraph 2, items 1, 2, 3, 4 and 11 of this Law.

(4) The Croatian Financial Services Supervision Agency shall conduct supervision of compliance with this Law with the reporting entities referred to in Article 4 paragraph 2, items 7, 8, 9 and 10 of this Law.

(5) The supervisory bodies referred to in Article 83, paragraph 1 shall be obliged to exchange data and information between each other needed for the supervisory procedures and to communicate the identified irregularities, should such findings be of relevance for the work of another supervisory body.

Section 3

REPORTING THE OFFICE ON THE CONDUCTED SUPERVISION

Reporting on the Identified Irregularities and Measures Taken

Article 86

(1) The supervisory bodies referred to in Article 83, paragraph 1, items b) to e) of this Law shall be obliged to notify the Office in writing without any undue delay, and no later than within 15 days, of the measures taken, the irregularities identified and other significant information, which shall be established through the minutes or other enactment of the supervisory body.

(2) The supervisory body referred to in paragraph 1 of this Article which established an infringement shall also notify other supervisory bodies of the results of its supervision, should the results be of relevance for their work in line with the signed agreements of understanding.

Reporting the Office by the Supervisory Bodies on Suspicion of Money Laundering or Terrorist Financing

Article 87

(1) The supervisory bodies referred to in Article 83, paragraph 1, items b) to e) of this Law shall be obliged to notify the Office in writing without any undue delay of information pointing to the relatedness of a person or a transaction with money laundering or terrorist financing, irrespective of whether they obtained such information during the course of carrying out supervision activities as per this Law or during the conducting of matters from their respective scopes of competence.

(2) In instances when bodies in charge of conducting supervision over the activities of non-profit organisations, save for supervisory bodies referred to in Article 83 of this Law, establish during the conducting of supervision from their scopes of competence that there shall exist reasons for suspicion of money laundering or terrorist financing in relation with the activity of a non-profit organisation, its members or persons related with them, they shall be obliged to notify the Office thereof in writing and without any undue delay

(3) In the cases referred to in paragraphs 1 and 2 of this Article, the Office shall, if it judges that there shall be grounds for suspicion of money laundering or terrorist financing, start collecting and analysing data, information and documentation in keeping with its tasks and scope of competence.

Issuing Recommendations and Guidelines

Article 88

In order for the reporting entities referred to in Article 4, paragraph 2 of this Law to be able to uniformly apply the provisions contained in this Law and the regulations passed on the basis of this Law, the supervisory bodies referred to in Article 83, paragraph 1 of this Law shall independently or in conjunction with other supervisory bodies issue recommendations or guidelines relative to the implementation of individual provisions contained in this Law and regulations passed on the basis of this Law

Competence for Running Misdemeanour Proceedings

Article 89

(1) The Financial Inspectorate of the Republic of Croatia shall make first-instance decisions on misdemeanours prescribed by this Law.

(2) Complaints may be filed with the High Misdemeanour Court of the Republic of Croatia against the decisions made by the Financial Inspectorate of the Republic of Croatia.

(3) The Financial Inspectorate is to furnish the Office with a copy of decisions taken in the first-instance and second-instance misdemeanour proceedings.

CHAPTER VII

PENAL PROVISIONS

Article 90

(1) A pecuniary penalty ranging from HRK 50,000.00 to HRK 700,000.00 shall be imposed on legal persons for the following infringements:

1. failure to develop a risk analysis, i.e. failure to make a risk assessment for individual groups or types of customers, business relationships, products or transactions or failure to make the risk analysis and assessment compliant with guidelines passed by the competent supervisory body (Article 7, paragraph 2, 3 and 5);
2. failure to apply the customer due diligence measures in instances prescribed by this Law (Article 9, paragraph 1 and Article 14, paragraph 4);
3. establishing a business relationship with a customer without conducting a prior customer due diligence (Article 10, paragraph 1);
4. conducting transactions valued at HRK 105,000.00 or greater, i.e. conducting mutually linked transactions reaching a total value of HRK 105,000.00 without prior conducting of the prescribed measures (Article 11);
5. failure to identify and verify customer's identity at customer's entry into a casino or at a point of conducting the transaction at the cash register or at registration of the customer to take part in the system of organising games of chance with the organiser who arrange games of chance on the Internet or other telecommunications means, i.e. electronic communications, i.e. for failure to obtain the prescribed customer information or failing to obtain such information in the prescribed manner (Article 12);
6. if, at conducting wire transfers or cash remittances, fails to collect or include in the form or a message accompanying a wire transfer in the prescribed manner accurate and valid data on

the sender, i.e. the order issuer, or if pertinent data fail to follow the transfer at all times throughout the course of the chain of payment (Article 15, paragraphs 1, 2);

7. if a payment services provider, acting as an intermediary or transfer receiver, fails to refuse a wire transfer which does not contain complete payee data or fails to supplement the payee data within a given deadline (Article 15, paragraphs 3);
8. failure to identify a customer or verify the customer's identity, i.e. the identity of a legal representative, a person authorised by power of attorney or the customer's beneficial owner, and failure to obtain documentation prescribed for the purposes of identification or identity verification or the power of attorney in instances when the customer shall conduct transactions by way of a person authorised by power of attorney (Articles 17, 18, 19, 20, 21 and 24);
9. failure to identify a customer or verify the customer's identity at customer's approaching a safe deposit box, i.e. failure to obtain the prescribed customer information or failure to obtain such information in the prescribed manner (Article 22);
10. failure to obtain data on the purpose and intended nature of a business relationship or a transaction within the framework of due diligence and other data required to be obtained as per this Law (Article 25);
11. establishing a business relationship with a customer in instances when the customer due diligence was conducted by a third person, contrary to this Law and the rulebook to be passed by the Minister of Finance (Article 28);
12. failure to conduct the prescribed measures and additionally obtain data, information and documentation or failure to obtain them in the prescribed manner at establishing a correspondent relationship with a bank or other credit institution seated in a third country (Article 31, paragraphs 1 and 3);
13. entering into or extending a correspondent relationship with a bank or other credit institution seated in a third country, contrary to the provisions contained in this Law (Article 31, paragraph 4);
14. failure to obtain data on the source of funds and property at entering into a business relationship with or conducting a transaction for a person who shall be foreign politically exposed person, which funds and property are or will be the subject matter of the business relationship or the transaction, or failure to obtain such data in the prescribed manner (Article 32, paragraph 7, item 1);
15. failure to apply one or several additional measures, in addition to the measures contained in Article 8, paragraph 1 of this Law, within the framework of the enhanced customer due diligence for the purpose of identification and identity verification of a customer who is not physically present (Article 33, paragraphs 1 and 2);
16. conducting a simplified customer due diligence under circumstances which shall mandatorily require the conducting of the enhanced due diligence because of entering into a correspondent relationship with a bank or other credit institution seated abroad (Article 31, paragraph 1 and Article 35, paragraph 2);
17. failure to obtain the required customer data within the framework of the simplified customer due diligence or failure to obtain such data in the prescribed manner (Article 36);
18. opening, issuing or keeping anonymous customer accounts, coded or bearer passbooks, i.e. accounts or passbooks in the name but containing no additional personal information or accounts registered at false names, i.e. other anonymous products (Article 37);
19. entering into or extending correspondent relationships with a bank which shall operate or might operate as a shell bank or with a credit institution known to enter account opening and keeping agreements with shell banks (Article 38);
20. receiving from a customer or a third person cash collection in an amount exceeding HRK 105,000.00, i.e. an amount exceeding EUR 15,000.00 in the arrangements with non-residents, i.e. receiving the collection in several mutually linked cash transactions jointly exceeding a total amount of HRK 105,000.00, i.e. exceeding the value of EUR 15,000.00 (Article 39, paragraphs 1 and 2);
21. failure to refrain from the conducting of a transaction for which the entity shall know or suspect to be connected with money laundering or terrorist financing, failure to notify the

Office of such transaction before its execution, and failure to indicate in the report the reasons for suspicion, the deadline within which the transaction is to be executed and other prescribed data or failure to notify the Office of the customer with which they terminated a business relationship or for whom they refused to conduct a transaction due to the inability to conduct the prescribed measures (Article 42 and Article 13, paragraph 2);

22. failure to supply the Office within the prescribed period with the required data, information and documentation on a transaction or a person for which there shall exist reasons for suspicion of money laundering or terrorist financing or failure to comply with the Office's authorised person's request to enable such a person exercise direct examination of the documentation at the legal person's business premises (Article 59, paragraphs 2, 3, 4, 5, 6, 7 and 9);
23. failure to comply with the temporary transaction suspension order as issued by the Office or failure to comply with the instruction on the course of action in relation to persons to which the temporary transaction suspension shall pertain (Article 60 and Article 71, paragraph 1);
24. failure to comply with the order for ongoing monitoring of a customer's financial operations as issued by the Office (Article 62, paragraphs 1, 2 and 3);
25. failure to close within the prescribed deadline the anonymous accounts and coded or bearer passbooks and all other anonymous products enabling the concealment of the customer identity, which were opened before the effective date of this Law or failure to conduct customer due diligence (Article 103).

(2) A pecuniary penalty ranging from HRK 6,000.00 to HRK 30,000.00 shall be imposed on members of management board or other legal person's responsible person for the infringements referred to in paragraph 1 of this Article.

(3) A pecuniary penalty ranging from HRK 35,000.00 to HRK 450,000.00 shall be imposed on a natural person craftsman or a natural person involved in other independent business activity for the infringements referred to in paragraph 1 of this Article.

Article 91

(1) A pecuniary penalty ranging from HRK 40,000.00 to HRK 600,000.00 shall be imposed on legal persons for the following infringements:

1. failure to ensure the conducting of the money laundering and terrorist financing detection and prevention measures defined in this law in its business units and subsidiaries seated in a third country (Article 5, paragraph 1);
2. failure to carry out all the prescribed customer due diligence measures or failure to carry them out in line with the procedure defined in their internal enactments and failure to define the measures conducting procedures in internal enactment (Article 8, paragraphs 1 and 2);
3. failure to obtain a written statement of a customer, the customer's legal representative or person authorised by power of attorney in instances when suspicion shall exist as to the veracity of data or credibility of documents serving as the foundation for identifying the customer, the customer's legal representative or the person authorised by power of attorney prior to the establishment of a business relationship or conducting a transaction (Article17, paragraph 5, Article 18, paragraph 5, Article 19, paragraph 2, Article 20, paragraph 5 and Article 21, paragraph 4);
4. failure to apply the prescribed measures in customer business activities monitoring (Article 26, paragraph 2);
5. failure to conduct a repeated annual foreign legal person customer due diligence, i.e. failure to obtain the prescribed data and documents or failure to obtain them in the prescribed manner (Article 27, paragraphs 1, 2, 3, 4, 5, 6 and 7);
6. conducting a transaction for a foreign legal person without conducting the repeated annual customer due diligence (Article 27, paragraph 8);

7. entrusting a third person with conducting the customer due diligence without checking whether or not such third person meets all the requirements prescribed by this Law (Article 28, paragraph 2);
8. accepting due diligence conducted by a third person as adequate, which third person conducted the customer identification and identity verification measure without the customer's physical presence (Article 28, paragraph 3);
9. entrusting a third person with conducting customer due diligence, which third person fails to meet requirements as prescribed in the rulebook to be passed by the Minister of Finance (Article 28, paragraph 6);
10. failure to provide for the foreign politically exposed persons identification procedure in its internal enactment (Article 32, paragraph 2);
11. failure to exercise due care monitoring of transactions and other business activities performed by a foreign politically exposed person with the legal person after entering into a business relationship with a person who shall be a politically exposed person (Article 32, paragraph 7, item 3);
12. establishing a business relationship with a customer who shall not be physically present at identification, without adopting a measure to ensure that the first payment be conducted through the account the customer has with the credit institution before the execution of any further customer's transaction (Article 33, paragraph 3);
13. for failure to put policies and procedures in place for monitoring the money laundering or terrorist financing risk which may stem from new technologies enabling anonymity (Internet banks, ATM use, tele-banking, etc.) or for failure to take measures aimed at preventing the use of new technologies for the money laundering and/or terrorist financing purposes (Article 34 paragraphs 1);
14. for failure to put policies and procedures in place for the risk attached with a business relationship or transactions with non face to face customers or for failure to apply them at the establishment of a business relationship with a customer and during the course of conducting customer due diligence measures (Article 34 paragraph 2).
15. failure to supply the Office within the prescribed period with data on a transaction being conducted in cash in an amount of HRK 200,000.00 or greater (Article 40, paragraph 1, 2 and 3);
16. failure to appoint the authorised person and one or several authorised person's deputies for the purpose of performing money laundering and terrorist financing detection and prevention matters, as laid down in this Law and regulations passed on the basis of this Law (Article 44);
17. failure to assign proper authorities to the authorised person and ensure the conditions for the performance of the authorised person's matters and tasks (Article 47);
18. failure to produce a list of indicators for the detection of customers and transactions for which there shall exist reasons for suspicion of money laundering or terrorist financing, or failure to produce such a list in the prescribed manner and within the prescribed period (Article 41, and Article 101, paragraph 2);
19. failure to pass an internal enactment providing for measures, actions and proceedings for the purpose of money laundering and terrorist financing prevention and detection, failure to provide for the responsibility of the authorised persons and other employees in charge of this Law implementation, and failure to supply the Office with a copy of the internal enactment at Office's request (Article 48);
20. failure to keep data and documentation during the period of ten years upon the transaction execution, i.e. the business relationship termination, the entry of a customer to a casino or approaching a safe deposit box (Article 78, paragraph 1);
21. failure to conduct a check of all existing customers within the prescribed period, in relation to which customers there shall or might exist a high money laundering or terrorist financing risk, in accordance with the provisions contained in article 7 of this Law (Article 102);
22. failure to stop correspondent relationships incompliant with the provisions contained in this Law within the prescribed period (Article 104).

(2) A pecuniary penalty ranging from HRK 3,000.00 to HRK 15,000.00 shall be imposed on members of management board or other legal person's responsible person for the infringements referred to in paragraph 1 of this Article.

(3) A pecuniary penalty ranging from HRK 15,000.00 to HRK 150,000.00 shall be imposed on a natural person craftsman or a natural person involved in other independent business activity for the infringements referred to in paragraph 1 of this Article.

Article 92

(1) A pecuniary penalty ranging from HRK 25,000.00 to HRK 400,000.00 shall be imposed on legal persons for the following infringements:

1. failure to notify the Office of the fact that legal regulations in force in a third country where business units or subsidiaries of the legal person shall be located shall not allow the conducting of money laundering detection and prevention measures to the extent prescribed in this Law, i.e. failure to pass adequate measures for the elimination of the money laundering or terrorist financing risk (Article 5, paragraph 2);
2. failure to familiarise their business units and companies in which they hold majority stake or majority decision-making right seated in a third country with internal procedures pertaining to money laundering and terrorist financing prevention and detection (Article 5, paragraph 3);
3. failure to examine the nature of the register of customer's registration at a point of verifying the identity of the legal person (Article 18, paragraph 6);
4. failure to ensure the alignment between the customer's business activities monitoring measures and the money laundering or terrorist financing risk the legal person shall be exposed to in conducting an arrangement or in doing business with a customer (Article 26, paragraph 3);
5. failure to use the list of indicators during establishing reasons for suspicion of money laundering or terrorist financing (Article 41, paragraph 3);
6. failure to supply the Office within the prescribed period with data on the appointment of the authorised person and the authorised person's deputy and any change thereof (Article 44, paragraph 2);
7. failure to make sure that the assignments of an authorised person and authorised person's deputy shall be performed by a person meeting the prescribed requirements (Article 45, paragraph 1);
8. failure to ensure regular professional development and training of all employees involved in the money laundering and terrorist financing prevention and detection matters as per this Law (Article 49, paragraph 1);
9. failure to produce an annual professional development and training plan pertinent to the money laundering and terrorist financing prevention and detection within the prescribed period (Article 49, paragraph 3);
10. failure to ensure regular internal audit of conducting the arrangements over the execution of money laundering and terrorist financing detection tasks as per this Law (Article 50);
11. failure to keep data and accompanying documentation on the authorised person and the authorised person's deputy, professional training of employees and the conducting of internal control within the prescribed period (Article 78, paragraph 2);
12. failure to keep records on customers, business relationships and transactions, and on the supplied data and examinations of data, information and documentation conducted by the supervisory bodies or for keeping inaccurate or incomplete records (Article 81, paragraphs 1, 3 and 6);

(2) A pecuniary penalty ranging from HRK 1,500.00 to HRK 8,000.00 shall be imposed on members of management board or other legal person's responsible person for the infringements referred to in paragraph 1 of this Article.

(3) A pecuniary penalty ranging from HRK 8,000.00 to HRK 80,000.00 shall be imposed on a natural person craftsman or a natural person involved in other independent business activity for the infringements referred to in paragraph 1 of this Article.

Article 93

(1) A pecuniary penalty ranging from HRK 50,000.00 to HRK 300,000.00 shall be imposed on a bank and other financial institutions should they fail to ensure within their respective computer systems such programme solutions to enable them to fully and timely respond to the requests of the Office (Article 6, paragraph 2, item 9).

(2) A pecuniary penalty ranging from HRK 3,000.00 to HRK 10,000.00 shall be imposed on members of management board or other legal person's responsible person for the infringements referred to in paragraph 1 of this Article.

Article 94

(1) A pecuniary penalty ranging from HRK 40,000.00 to HRK 400,000.00 shall be imposed on a legal person who performed customer due diligence in lieu of the reporting entity, should it fail to report the Office of the transactions in relation to which there shall exist suspicion of money laundering or terrorist financing or should it be incompliant with the requirement of keeping data and documentation prescribed by this Law (Article 28, paragraph 4).

(2) A pecuniary penalty ranging from HRK 3,000.00 to HRK 15,000.00 shall be imposed on members of management board or other legal person's responsible person for the infringements referred to in paragraph 1 of this Article.

Article 95

(1) A pecuniary penalty ranging from HRK 1,500.00 to HRK 8,000.00 shall be imposed on a responsible person who shall enter into a correspondent relationship on behalf of the reporting entity with a bank or a similar credit institution seated in a third country without obtaining a prior written consent from the superior (Article 31, paragraph 2).

(2) A pecuniary penalty ranging from HRK 1,500.00 to HRK 8,000.00 shall be imposed on a responsible person who shall establish a business relationship on behalf of the reporting entity with a customer who shall be a politically exposed person without obtaining a prior written consent from the superior (Article 31, paragraph 7, item 2).

(3) A pecuniary penalty ranging from HRK 15,000.00 to HRK 80,000.00 shall be imposed on a bank or other legal person on whose behalf the responsible person entered into an agreement or established another business relationship for the infringements referred to in paragraphs 1 and 2 of this Article.

Article 96

(1) A pecuniary penalty ranging from HRK 60,000.00 to HRK 400,000.00 shall be imposed on an auditing firm and an independent auditor, should they conduct a simplified customer due diligence in spite of the fact that there shall exist reasons for suspicion of money laundering or terrorist financing in relation to a customer or circumstances of an audit (Article 53, paragraph 8).

(2) A pecuniary penalty ranging from HRK 6,000.00 to HRK 30,000.00 shall be imposed on members of management board of or other responsible person in the auditing firm or a firm rendering accounting services or tax advisory services for the infringements referred to in paragraph 1 of this Article.

Article 97

(1) A pecuniary penalty ranging from HRK 50,000.00 to HRK 300,000.00 shall be imposed on a lawyer, a law firm, a notary public, an auditing firm, an independent auditor, as well as a legal and a natural person rendering accounting services or tax advisory services for the following infringements:

1. failure to obtain all prescribed data within the framework of customer due diligence, i.e. failure to obtain all prescribed data or data on the purpose and intended nature of the business relationship or the transaction, data on the source of money or other prescribed data (Article 53, paragraphs 1, 2 and 3);
2. failure to identify the customer, i.e. a customer's legal representative, a person authorised by power of attorney or the beneficial owner or for failure to gather information of these persons' identity in the prescribed manner (Article 53, paragraph 4);
3. failure to notify the Office within the prescribed period or in the prescribed manner concerning a transaction, an intended transaction or a customer in relation to which there shall exist reasons for suspicion of money laundering or terrorist financing (Article 54, paragraphs 1 and 3);
4. failure to notify the Office within the deadlines of a customer who sought for a money laundering or terrorist financing related advice (Article 54, paragraph 2);
5. failure to notify the Office of a cash transaction under circumstances in which there shall exist reasons for suspicion of money laundering or terrorist financing in relation with the transaction or customer (Article 55, paragraph 3);
6. failure to comply with the request of the Office to supply the required data information and documentation within the prescribed deadline in relation with a transaction or a person for which the Office had judged that there shall exist reasons for suspicion of money laundering or terrorist financing (Article 59, paragraphs 2, 5, 6 and 7);
7. failure to keep data obtained on the basis of Article 53 of this Law and the accompanying documentation for the period of ten years after the conducting of customer due diligence (Article 78, paragraph 3).

(2) A pecuniary penalty ranging from HRK 30,000.00 to HRK 200,000.00 shall be imposed on a lawyer, a law firm, a notary public, an auditing firm, an independent auditor, as well as a legal and a natural person rendering accounting services or tax advisory services for the following infringements:

1. failure to identify the beneficial owner of a customer which shall be a legal person or a similar entity subject to foreign law, i.e. failure to obtain the prescribed data or failure to obtain them in the prescribed manner (Article 53, paragraphs 5, 6 and 7);
2. failure to produce a list of indicators for the detection of customers and transaction for which there shall exist reasons for suspicion of money laundering or terrorist financing or failure to produce the list of indicators in the prescribed manner or within the prescribed deadline (Article 41 and Article 101, paragraph 2);
3. failure to supply the Office with data, information and documentation within the prescribed deadline and in the prescribed manner concerning the performance of their assignments as per this Law or other data necessary for conducting supervision (Article 59, paragraphs 3, 4, 5, 6 and 7).

(3) A pecuniary penalty ranging from HRK 25,000.00 to HRK 180,000.00 shall be imposed on a lawyer, a law firm, a notary public, an auditing firm, an independent auditor, as well as a legal and a natural person rendering accounting services or tax advisory services for the following infringements:

1. failure to provide regular professional development and training of employees involved in the performance of money laundering and terrorist financing prevention and detection matters as per this Law (Article 49, paragraph 1);
2. failure to develop an annual professional development and training plan in the filed of money laundering and terrorist financing prevention and detection field within the prescribed deadline (Article 49, paragraph 3);
3. failure to notify the Office in writing of reasons for the non-observance of a request for the supply of data, information and documentation on a transaction or a customer in relation with

which there shall exist reasons for suspicion of money laundering or terrorist financing or failure to do so within the prescribed deadline (Article 55, paragraph 2);
4. failure to use the list of indicators at establishing reasons for suspicion of money laundering or terrorist financing and other circumstances thereof (Article 41, paragraph 3);
5. failure to keep data and accompanying documentation on professional training for the period of four years after the training delivery (Article 78, paragraph 4);
6. failure to keep records on customers, business relationships and transactions, as well as on the supplied data and the conducting of examinations of supervisory bodies of data, information and documentation, i.e. for keeping inaccurate or incomplete records (Article 81, paragraphs 2 and 3);

(4) A pecuniary penalty ranging from HRK 5,000.00 to HRK 20,000.00 shall be imposed on members of management board or other legal person's responsible person for the infringements referred to in paragraphs 1, 2 and 3 of this Article.

Article 98

A pecuniary penalty ranging from HRK 10,000.00 to HRK 50,000.00 shall be imposed on a responsible person in a state administration body or in a local and regional self-government unit should they fail to supply the Office within the prescribed deadline and in the prescribed manner with the requested data, information and the documentation required by the Office for supervisory purposes (Article 63, paragraph 3).

Article 99

(1) In instances when a special law shall envisage the issuance of an approval for the performance of certain arrangements, the competent body shall be entitled to recall the approval for the performance of such arrangements from legal or natural persons in breach of the provisions contained in this Law.

(2) The measure referred to in paragraph 1 of this Article may be applied for the period of three months to one year.

Article 100

(1) The misdemeanour proceedings for the infringements envisaged by this Law may not be commenced after the expiration of three years from the date of the infringement.

(2) The statute of limitations shall become effective in all instances when there shall expire six years after the infringement.

CHAPTER VIII

TRANSITIONAL AND FINAL PROVISIONS

Bylaws and the List of Indicators

Article 101

(1) The Minister of Finance shall undertake to pass the regulations under his remit as per this Law within a maximum period of 6 months after this Law enters into force.

(2) The reporting entities referred to in Article 4, paragraph 2 of this Law shall undertake to produce a list of indicators for the detection of suspicious transactions and customers in relation to which reasons for suspicion of money laundering and terrorist financing shall exist no later than within three months after the effective date of this Law.

(3) The list of indicators for the detection of suspicious transactions and customers in relation to which reasons for suspicion of money laundering and terrorist financing shall exist that the reporting

entities referred to in Article 4, paragraph 2 of this Law had applied on the basis of the Anti-Money Laundering Law (Official Gazette of the Republic of Croatia Narodne novine No. 69/97, 106/97, 67/01, 114/01, 117/03 and 142/03) and the Rulebook on the Anti-Money Laundering Law Implementation (Narodne novine No. 189/03) shall remain in force until the passage of the list referred to in paragraph 2 of this Article.

Existing Customers Due Diligence

Article 102

The reporting entities referred to in Article 4, paragraph 2 of this Law shall undertake to conduct due diligence of all existing customers within one year after the effective date of this Law, for which existing customers the reporting entities shall establish on the basis of Article 7 of this Law that a money laundering or terrorist financing risk shall or might exist.

Compliance in terms of Anonymous Products

Article 103

(1) The reporting entities shall be obliged to close all anonymous accounts, coded or bearer passbooks as well as all other anonymous products, including accounts registered to false names that directly or indirectly enable the concealment of customers' identity within 30 days upon the effective date of this Law.

(2) By way of derogation from the provisions contained in Article 37 of this Law, for those anonymous accounts, coded or bearer passbooks as well as all other anonymous products, including accounts registered to false names whose owners may not be established, and which anonymous products shall exist at the effective date of this Law, the reporting entities shall be obliged to conduct customer or other product user due diligence, in keeping with the provisions of Article 8 of this Law, during the first transaction that the customer or another user shall conduct on the basis of such products.

Compliance of the Reporting Entities

Article 104

The reporting entities shall undertake to make their operations compliant with the provisions contained in Article 38 of this Law within the period of the six months from the effective date of this Law.

Effects of the Law entry into force

Article 105

(1) With the effective date of this Law, the Anti-Money Laundering Law (Official Gazette of the Republic of Croatia Narodne novine No. 69/97, 106/97, 67/01, 114/01, 117/03 and 142/03) shall become null and void.

(2) The Rulebook on the Anti-Money Laundering Law Implementation (Official Gazette of the Republic of Croatia Narodne novine No. 189/03) shall remain in force until the passage of regulations referred to in Article 101, paragraph 1 of this Law, in the sections not contrary to the provisions of this Law.

Entry into Force

Article 106

This Law shall be published in the Official Gazette of the Republic of Croatia Narodne novine, and shall enter into force as at 1 January 2009.

Class: 215-01/08-01/01
Zagreb, 15 July 2008

CROATIAN PARLIAMENT

Speaker of the
Croatian Parliament
Luka Bebic, signed

ANNEX III Criminal Act 2011

Application of Criminal Legislation to Criminal Offences Committed Aboard a Vessel or Aircraft of the Republic of Croatia

Article 11

The criminal legislation of the Republic of Croatia shall also be applied to anyone who commits a criminal offence aboard a national vessel or aircraft, irrespective of where the vessel or the aircraft is located at the time the criminal offence was committed.

Particularities Concerning the Institution of Criminal Proceedings for Criminal Offences Committed in the Territory of the Republic of Croatia, Aboard its Vessel or Aircraft

Article 12

(1) Where, in the case of application of the criminal legislation of the Republic of Croatia pursuant to the provisions of Articles 10 and 11 of this Act, criminal proceedings in a foreign country have ended with a judgment having the force of *res judicata*, criminal proceedings in the Republic of Croatia shall be instituted upon authorisation from the State Attorney.

(2) Criminal proceedings for the purpose of applying the criminal legislation of the Republic of Croatia pursuant to the provisions of Articles 10 and 11 of this Act shall not be instituted against the perpetrator of a criminal offence which, besides in the territory of the Republic of Croatia, was also committed in the territory of a signatory state to the Convention implementing the Schengen Agreement, in which country the criminal proceedings for this criminal offence have ended with a judgment having the force of *res judicata*.

Application of Criminal Legislation to Criminal Offences Committed against a Legal Interest of the Republic of Croatia outside its Territory

Article 13

The criminal legislation of the Republic of Croatia shall be applied to anyone who, outside its territory, commits:

1. a criminal offence against the Republic of Croatia provided for in Title XXXII of this Act,
2. the criminal offence of counterfeiting money, securities and value signs of the Republic of Croatia as defined in Articles 274, 275 and 276 of this Act,
3. a criminal offence against a Croatian state official or a government employee relating to his/her office,
4. a criminal offence of false testimony referred to in Article 305 of this Act if the false testimony was given in proceedings before Croatian competent authorities,
5. criminal offences against the right to vote referred to in Title XXXI of this Act,
6. a criminal offence referred to in Articles 193, 194, 196, 197 and 198 of this Act when committed in the ecological and fisheries protection zone, epicontinental belt or in open sea.

Application of Criminal Legislation to Criminal Offences Committed Outside the Territory of the Republic of Croatia by its Citizens

Article 14

(1) The criminal legislation of the Republic of Croatia shall be applied to a Croatian citizen or a person with permanent residence in the Republic of Croatia who outside the territory of the Republic of Croatia commits a criminal offence other than those established in accordance with the provisions of Articles 13 and 16 of this Act, provided the criminal offence in question is also punishable under the law of the country in which it was committed.

(2) The provision of paragraph 1 of this Article shall also be applied to cases where the perpetrator acquires Croatian citizenship after having committed the criminal offence.

(3) In cases referred to in paragraphs 1 and 2 of this Article, with respect to criminal offences referred to in Article 115, paragraphs 3 and 4, and Articles 116, 153, 154, 158, 161, 162, 163, 164, 166 and 169 of this Act and other criminal offences provided for by international treaties to which the Republic of Croatia is a party, the criminal legislation of the Republic of Croatia shall also be applied to cases where the criminal offence is not punishable under the law of the country in which it was committed.

(4) Where a Croatian citizen participates in peacekeeping operations or other international activities outside of the territory of the Republic of Croatia and commits in such operations or activities a criminal offence, the application of the legislation of the Republic of Croatia shall be governed by the provisions of this Act, unless otherwise provided by an international treaty to which the Republic of Croatia is a party.

Application of Criminal Legislation to Criminal Offences Committed against the Citizens of the Republic of Croatia Outside its Territory

Article 15

(1) The criminal legislation of the Republic of Croatia shall be applied to an alien who outside the territory of the Republic of Croatia commits a criminal offence other than those established in accordance with the provisions of Articles 13 and 16 of this Act against a citizen of the Republic of Croatia, a person with a permanent residence in the Republic of Croatia or a legal person registered in the Republic of Croatia, provided the criminal offence in question is also punishable under the law of the country in which it was committed.

(2) In the case referred to in paragraph 1 of this Article, the court may not impose a penalty more severe that the one prescribed by the law of the country in which the criminal offence was committed.

Application of Criminal Legislation to Criminal Offences against Values Protected by International Law, Committed outside the Territory of the Republic of Croatia

Article 16

The criminal legislation of the Republic of Croatia shall be applied to anyone who outside its territory commits any of the criminal offences referred to in Articles 88, 90, 91, 97, 104, 105 and 106 of this Act or a criminal offence which the Republic of Croatia is required to punish under an international treaty also when committed outside the territory of the Republic of Croatia.

Application of Criminal Legislation to Other Criminal Offences Committed outside the Territory of the Republic of Croatia

Article 17

(1) The criminal legislation of the Republic of Croatia shall be applied to an alien who outside the territory of the Republic of Croatia commits a criminal offence for which a sentence of imprisonment of five years or a more severe punishment may be imposed under the Croatian law, where this does not concern the cases referred to in Articles 13 through 16 of this Act, provided the criminal offence in question is also punishable under the law of the country in which it was committed and that the extradition of the perpetrator is permitted under the law or an international treaty but has not come to pass.

(2) With respect to the case referred to in paragraph 1 of this Article, the court may not pronounce a sentence that is more severe than the one provided for by the law of the country in which the criminal offence was committed.

Particularities Concerning the Institution of Criminal Proceedings for Criminal Offences Committed outside the Territory of the Republic of Croatia

Article 18

(1) Where, in the case of application of the criminal legislation in the Republic of Croatia pursuant to provisions of Article 13 of this Act, criminal proceedings have ended with a judgment having the force of *res judicata* in a foreign country, the State Attorney General may desist from criminal prosecution.

(2) In cases referred to in Articles 14, 15 and 17 of this Act, criminal proceedings for the purpose of applying the criminal legislation of the Republic of Croatia shall not be instituted:

1. if the *res judicata* sentence has been carried out or is in the process of being carried out or can no longer be carried out under the law of the country in which the person was convicted,

2. if the perpetrator has been acquitted by a judgment having the force of *res judicata* in a foreign country or if he/she has been granted pardon under the law of the country in which he/she committed the criminal offence,

3. if under the law of the country in which the criminal offence was committed, the criminal offence in question is prosecuted on the basis of a motion or private action, and such motion or private action have not been filed, or the statute of limitations for criminal prosecution has expired.

(3) In the case referred to in Article 16 of this Act, criminal proceedings for the purpose of applying criminal legislation of the Republic of Croatia may be instituted provided that criminal prosecution has not been initiated before the International Criminal Court or a court of another country or that just proceedings before a court of the country in which the criminal offence was committed, a court of the country of which the perpetrator is a citizen or another court with jurisdiction to adjudicate cannot be expected. If criminal proceedings were carried out in another country contrary to internationally recognised standards of just adjudication, criminal proceedings may be instituted only with the authorisation from the State Attorney General.

(4) In the case referred to in Articles 14, 15, 16 and 17 of this Act criminal proceedings shall be instituted only if the perpetrator is located in the territory of the Republic of Croatia.

Crediting Time Spent Deprived of Liberty and Criminal-Law Sanctions Executed in a Foreign Country

Article 19

Where criminal legislation of the Republic of Croatia is applied, time spent in custody, remand or serving one's sentence, as well as any other deprivation of liberty in a foreign country shall be credited towards the length of the pronounced sentence of imprisonment handed down by a national court for the same criminal offence. Other executed criminal-law sanctions shall be credited according to a just assessment by the court.

Intent

Article 28

(1) A criminal offence may be committed with direct (*dolus directus*) or indirect intent (*dolus eventualis*).

(2) A perpetrator is acting with direct intent when he/she is aware of the elements of a criminal offence and wants or is certain of their realisation.

(3) A perpetrator is acting with indirect intent when he/she is aware that he/she is capable of realising the elements of a criminal offence and agrees to this.

Mistake as to the Elements Constituting an Offence

Article 30

(1) Whoever at the time of commission of an offence is not aware of one of its statutory elements is not acting with intent.

(2) If the mistake referred to in paragraph 1 was avoidable, the perpetrator shall be punished for negligence where the law also prescribes punishment for the commission of an offence by negligence.

Attempt

Article 34

(1) Whoever, with the intent to commit a criminal offence, performs an act which spatially and temporally directly precedes the realisation of the statutory definition of the criminal offence shall be punished for the attempt, provided that a sentence of imprisonment of five years or a more severe punishment may be imposed or that the law expressly provides for the punishment of an attempt as well.

(2) The perpetrator of an attempt may be punished less severely.

(3) The punishment of a perpetrator who through gross unreasonableness attempts to commit a criminal offence by unsuitable means or towards an unsuitable object may be remitted.

Perpetratorship

Article 36

(1) A perpetrator is a person who by himself/herself or via another person commits a criminal offence.

(2) If on the basis of a joint decision a number of persons commit a criminal offence so that each one of them participates in the carrying out of the act or otherwise substantially contributes to the commission of the criminal offence, each one of them shall be punished as the perpetrator (accomplices).

(3) Negligent liability of accomplices is based on a joint violation of due care.

Incitement

Article 37

(1) Whoever intentionally incites another to commit a criminal offence shall be punished as if he/she himself/herself has committed it.

(2) Whoever intentionally incites another to commit a criminal offence for which an attempt is punishable, and the act is never even attempted, shall incur the penalty provided for an attempt to commit this criminal offence.

(3) In the case of an inappropriate attempt at incitement, the punishment of the inciter may be remitted.

Aiding

Article 38

Whoever intentionally aids another in the commission of a criminal offence may be punished less severely.

Punishment of Accomplice and Participant

Article 39

(1) Every accomplice and participant (inciter and aider) shall be punished according to his/her guilt.

(2) Special personal circumstances by reason of which the law provides for remission or mitigation of punishment or for a less serious or a more serious form of criminal offence shall be taken into account only with respect to the accomplice or participant in whose person they are present.

Conditions for and Manner of Confiscation of Pecuniary Advantage

Article 77

(1) Pecuniary advantage shall be confiscated on the basis of a court decision establishing the commission of an unlawful act. Pecuniary advantage shall also be confiscated from the person to whom it was transferred if it was not acquired in good faith.

(2) If the injured party has been awarded a pecuniary claim which by its nature and contents corresponds to the acquired pecuniary advantage, the part of pecuniary advantage exceeding the awarded pecuniary claim shall be confiscated.

(3) The court shall confiscate the pecuniary advantage also in cases where it has instructed the injured party to assert his/her pecuniary claim in a civil action.

(4) Where it has been established that confiscation in full or in part of things or rights acquired as pecuniary advantage is impossible, the court shall order the perpetrator to pay the corresponding money equivalent. It may be ordered that payment be made in instalments.

(5) The confiscated pecuniary advantage shall not be reduced by the value of resources invested in the criminal activity.

(6) The court may decide against the confiscation of pecuniary advantage if its value is negligible.

MEANING OF TERMS USED IN THIS ACT

Article 87

(1) The criminal legislation of the Republic of Croatia shall mean the provisions contained in this Act and other acts of the Republic of Croatia determining the conditions for punishability and the sanctions that may be imposed on the perpetrators of criminal offences.

(2) An unlawful act shall mean an act having the elements of a criminal offence, provided no reason for excluding unlawfulness exists.

(3) An official person shall mean a high-ranking or a lower-ranking state official, a high-ranking or a lower-ranking official in a unit of the local or regional self-government, holder of judicial authority, lay judge, member of the State Judiciary Council or the State Attorney's Council, arbitrator, notary public and bailiff. An official person shall also mean a person who in the European Union, another state, international organisation of which the Republic of Croatia is a member, international tribunal or arbitration board the jurisdiction of which the Republic of Croatia accepts, performs the duties confided to persons listed in the previous sentence.

(4) A member of the armed forces shall mean a person on active duty in the armed forces, a conscript, a reservist, a cadet and a lower-ranking state official and state employee assigned to a post in the armed forces of the Republic of Croatia.

(5) When an official person is designated as the perpetrator of a criminal offence not provided for in Title XXXIV of this Act or as a person against whom a criminal offence has been committed, a member of the armed forces shall also be considered an official person.

(6) A responsible person shall mean a physical person conducting the affairs of a legal person or a physical person to whom the running of affairs from the legal person's sphere of activity has expressly or effectively been confided.

(7) A child shall mean a person who has not attained the age of eighteen years.

(8) Family members shall mean the current spouse or cohabitant, their children and children of either of them, lineal blood relative, collateral blood relatives up to the third degree of kinship, in-laws up to the second degree in the conjugal community or cohabitation, adopter and adoptee, adopter's lineal blood relatives, adopter's collateral blood relatives up to the third degree of kinship, adopter's in-laws up to the second degree of kinship. In the case of criminal offences of domestic violence, family members under this Act shall also mean a former spouse or cohabitant, children of either of them and their children if former conjugal or extramarital relations were the source of conflict after the termination of a conjugal relationship or cohabitation, persons having children together, guardian and ward, foster parent, beneficiary of accommodation in a foster family and members of their family during such a relationship, child and person who has taken the child into care and who is responsible for his/her upbringing. Protection shall also be provided to the same-sex partner and children of either of them or a former same-sex partner and the children of either of them under the same terms and conditions as those that apply to family members or persons considered family members under this Act.

(9) A cohabitant shall mean a person living in a cohabiting relationship of a more lasting character or in which a child is born.

(10) A same-sex partner shall mean a person living in a same-sex partnership of a more lasting character.

(11) A secret piece of information shall mean a piece of information designated as a classified piece of information under a special act. A secret piece of information shall not mean a piece of information whose contents are contrary to the constitutional order of the Republic of Croatia or which has been designated as secret for the purpose of covering-up a criminal offence, exceeding or abusing authority or other forms of illegal actions in state bodies.

(12) An official secret shall mean a piece of information collected and used for the needs of public authority bodies which pursuant to an act, another regulation or a general act of a competent body adopted on the basis of an act has been declared an official secret, provided that it is not a classified piece of information under a special act.

(13) Elections shall mean elections for the Croatian Parliament, presidential elections, elections for the European Parliament, representative bodies in the units of local and regional self-government, elections of mayors, city mayors, prefects, the Zagreb City mayor and the decision-making process in the national referendum.

(14) A document shall mean any object containing an inscription, sign or picture which is suitable or has been chosen to serve as evidence of a particular fact that is of value for legal relations.

(15) A piece of moveable property shall also mean any manufactured or collected energy for the giving of light, heat or motion, as well as telephone impulses.

(16) A motor vehicle shall mean any motor-driven means of transport by road, water or air.

(17) A computer system shall mean any device or a group of inter-connected or inter-linked devices, one or more of which process data automatically on the basis of a computer programme, as well as computer data stored or processed in, read or transferred into it for the purpose of its operation, use, protection and maintenance.

(18) Computer data shall mean any denotation of facts, information or ideas in a form suitable for computer processing.

(19) A computer programme shall mean a set of computer data that are capable of prompting the computer system to perform a certain function.

(20) A hate crime shall mean a criminal offence committed on account of a person's race, colour, religion, national or ethnic origin, disability, gender, sexual orientation or gender identity. Unless a more severe penalty is explicitly prescribed by this Act, such conduct shall be taken as an aggravating circumstance.

(21) A pecuniary advantage obtained by a criminal offence shall mean a direct pecuniary advantage obtained by a criminal offence consisting of any increase or prevention of decrease in the property which came about as a result of the commission of a criminal offence, the property into which the direct pecuniary advantage obtained by a criminal offence has been changed or turned into as well as any other advantage gained from the direct pecuniary advantage obtained by a criminal offence or from property into which the direct pecuniary advantage gained by a criminal offence has been changed or turned into, irrespective of whether it is located inside or outside the territory of the Republic of Croatia.

(22) A bribe shall mean any reward, gift or another undue pecuniary or non-pecuniary advantage, irrespective of its value.

(23) A victim of a criminal offence shall mean a physical person who by an unlawful act has been inflicted physical or mental pain, emotional suffering, has suffered damage to his/her property or against whom a serious violation of human rights and fundamental freedoms has been committed.

Genocide

Article 88

(1) Whoever with intent to destroy, in whole or in part, a national, ethnical, racial or religious group, as such:

1. kills members of the group;

2. causes serious bodily harm to or severely undermines the health of members of the group;

3. deliberately inflicts on the group conditions of life calculated to bring about its physical destruction in whole or in part;

4. imposes measures intended to prevent births within the group; or

5. forcibly transferring children to another group

shall be sentenced to imprisonment for a term of at least ten years or to long-term imprisonment.

(2) Whoever orders the commission of genocide shall be imposed the sentence referred to in paragraph 1 of this Article.

(3) Whoever directly and publicly incites to the commission of genocide

shall be sentenced to imprisonment for a term of between one and ten years.

Crime of Aggression

Article 89

(1) Whoever, being in a position effectively to exercise control over or to direct the political or military action of a state, uses the armed forces of one state against the sovereignty, territorial integrity or political independence of another state, or in any other manner inconsistent with the Charter of the United Nations executes an act of aggression which, by its character, gravity and scale, constitutes a violation of the Charter of the United Nations shall be sentenced to imprisonment for a term of at least five years or to long-term imprisonment.

(2) Whoever takes part in the operations of the armed forces referred to in paragraph 1 of this Article shall be sentenced to imprisonment for a term of between three to fifteen years.

(3) Whoever directly and publicly incites to the crime of aggression shall be sentenced to imprisonment for a term of between one and ten years.

(4) Any of the following acts, regardless of a declaration of war, shall qualify as an act of aggression referred to in paragraph 1 of this Article:

1. The invasion or attack by the armed forces of a state on the territory of another state, or any military occupation, however temporary, resulting from such invasion or attack, or any annexation by the use of force of the territory of another state or part thereof;

2. bombardment by the armed forces of a state against the territory of another state or the use of any weapons by a state against the territory of another state;

3. the blockade of the ports or coasts of a state by the armed forces of another state;

4. an attack by the armed forces of a state on the land, sea or air forces, or marine and air fleets of another state;

5. the use of armed forces of one state which are within the territory of another state with the agreement of the receiving state, in contravention of the conditions provided for in the agreement or any extension of their presence in such territory beyond the termination of the agreement;

6. the action of a state in allowing its territory, which it has placed at the disposal of another state, to be used by that other state for perpetrating an act of aggression against a third state; or

7. the sending by or on behalf of a state of armed bands, groups, irregulars or mercenaries, which carry out acts of armed force against another state of such gravity as to amount to the acts listed above, or its substantial involvement therein.

Crime against Humanity

Article 90

(1) Whoever, in violation of the rules of international law, as part of a widespread or systematic attack directed against any civil population, with knowledge of the attack:

1. kills another person;

2. for the purpose of extermination inflicts on a civilian population conditions of life calculated to bring about the destruction of part of the population;

3. enslaves a person by exercising any or all of the powers attaching to the right of ownership over the person, including the exercise of such power in the course of trafficking in persons;

4. deports or forcibly transfers the persons concerned by expulsion or other coercive acts from the area in which they are lawfully present, without grounds permitted under international law;

5. unlawfully imprisons another person or otherwise unlawfully deprives the person of physical liberty;

6. tortures a person in the custody or under the control of the accused by intentionally inflicting upon the person severe pain or suffering, whether physical or mental, except such pain or suffering arising only from, inherent in or incidental to, lawful sanctions;

7. rapes another person, holds another person in sexual slavery, forces him/her into prostitution, unlawfully confines a woman forcibly made pregnant with the intent of affecting the ethnic composition of any population or carrying out other grave violations of international law, without the consent of another person and when this is not justified by medical reasons sterilises the person or inflicts on him/her any other form of sexual violence of comparable gravity;

8. persecutes any identifiable group or collectivity on political, racial, national, ethnic, cultural, religious, gender or other grounds that are universally recognised as impermissible under international law, and does this in connection with any act described in Articles 88 through 91 of this Act, by intentionally and severely depriving another person of fundamental rights contrary to international law by reason of his/her belonging to a certain group or collectivity;

9. arrests, detains or abducts persons on behalf of or with the authorisation, support or acquiescence of, a state or political organisation, followed by a refusal to acknowledge that deprivation of liberty or to give information on the fate or whereabouts of those persons, with the intention of removing them from the protection of the law for a prolonged period of time;

10. in the context of an institutionalised regime of systematic oppression and domination by one racial group over any other racial group or groups and with the intention of maintaining that regime commits an inhumane act described in this Article or an act similar to any of these acts (crime of apartheid); or

11. commits other inhumane acts of a similar character intentionally causing great suffering, or serious injury to the body or to mental or physical health

shall be sentenced to imprisonment for a term of at least five years or to long-term imprisonment.

(2) The sentence referred to in paragraph 1 of this Article shall be imposed on the person who orders any of the above criminal offences.

War Crime

Article 91

(1) Whoever, in violation of the rules of international law, in times of war, occupation, international armed conflict or non-international armed conflict commits any of the following grave violations against persons or property protected under the Geneva Conventions of 12 August 1949:

1. killing;
2. torture or inhuman treatment, including biological experiments;
3. causing great suffering, or serious injury to body or health;
4. unlawful deportation or transfer or unlawful confinement of a protected person;
5. compelling a prisoner of war or other protected person to serve in the forces of a hostile power;
6. wilfully depriving a prisoner of war or other protected person of the rights of fair and regular trial;
7. taking of hostages; or

8. extensive destruction and appropriation of property, not justified by military necessity and carried out unlawfully and wantonly

shall be sentenced to imprisonment for a term of at least five years or to long-term imprisonment.

(2) Whoever, in violation of the rules of international law, in times of war, occupation, international armed conflict or non-international armed conflict commits other serious violations of the laws and customs applicable in international armed conflict or non-international armed conflict, within the established framework of international law, namely, any of the following acts:

1. directing attacks against the civilian population as such or against individual civilians not taking direct part in hostilities;

2. directing attacks against civilian objects, that is, objects which are not military objectives;

3. directing attacks against personnel, installations, material, units or vehicles involved in a humanitarian assistance or peacekeeping mission in accordance with the Charter of the United Nations, as long as they are entitled to the protection given to civilians or civilian objects under the international law of armed conflict;

4. launching an attack in the knowledge that such attack will cause incidental loss of life or injury to civilians or damage to civilian objects or widespread, long-term and severe damage to the natural environment which would be clearly excessive in relation to the concrete and direct overall military advantage anticipated;

5. attacking or bombarding, by whatever means, towns, villages, dwellings or buildings which are undefended and which are not military objectives;

6. killing or wounding a combatant who, having laid down his arms or having no longer means of defence, has surrendered at discretion;

7. making improper use of a flag of truce, of the flag or of the military insignia and uniform of the enemy or of the United Nations, as well as of the distinctive emblems of the Geneva Conventions, resulting in death or serious personal injury;

8. the transfer, directly or indirectly, by the occupying power of parts of its own civilian population into the territory it occupies, or the deportation or transfer of all or parts of the population of the occupied territory within or outside this territory;

9. directing attacks against buildings dedicated to religion, education, art, science or charitable purposes, historic monuments, hospitals and places where the sick and wounded are collected, provided they are not military objectives;

10. subjecting persons who are in the power of an adverse party to physical mutilation, the taking of tissues or organs for transplantation or to medical or scientific experiments of any kind which are neither justified by the medical, dental or hospital treatment of the person concerned nor carried out in his or her interest, and which cause death to or seriously endanger the health of such person or persons;

11. killing or wounding treacherously individuals belonging to the hostile nation or army;

12. declaring that no quarter will be given;

13. destroying or seizing the enemy's property unless such destruction or seizure be imperatively demanded by the necessities of war;

14. declaring prohibited, suspended or inadmissible in a court of law the rights and actions of the nationals of the hostile party;

15. compelling the nationals of the hostile party to take part in the operations of war directed against their own country, even if they were in the belligerent's service before the commencement of the war;

16. pillaging a town or place;

17. employing poison or poisoned weapons;

18. employing asphyxiating, poisonous or other gases, and all analogous liquids, materials or devices;

19. employing bullets which expand or flatten easily in the human body;

20. employing weapons, projectiles and material and methods of warfare which are of a nature to cause superfluous injury or unnecessary suffering or which are inherently indiscriminate in violation of the international law of armed conflict, provided that such weapons, projectiles and material and methods of warfare are the subject of a comprehensive prohibition;

21. committing outrages upon personal dignity, in particular humiliating and degrading treatment, collective punishment;

22. committing rape, sexual slavery, enforced prostitution, forced pregnancy, enforced sterilisation, or any other form of sexual violence also constituting a grave breach of the Geneva Conventions;

23. utilizing the presence of a civilian or other protected person to render certain points, areas or military forces immune from military operations;

24. directing attacks against buildings, material, medical units and transport, and personnel using the distinctive emblems of the Geneva Conventions in conformity with international law;

25. intentionally using starvation of civilians as a method of warfare by depriving them of objects indispensable to their survival, including impeding relief supplies as provided for under the Geneva Conventions;

26. conscripting or enlisting children into the national armed forces or armed groups distinct from the national armed forces or using them to participate actively in hostilities; or

27. displacing the civilian population for reasons connected with the conflict, unless their security or imperative military reasons so demand

shall be sentenced to imprisonment for a term of at least three years.

(3) The sentence referred to in paragraph 1 of this Article shall be imposed on anyone who commits any of the crimes set out in paragraph 2 of this Article against a great many persons or in an especially cruel or treacherous way, for love of gain or other base motives.

(4) Whoever orders the commission of a crime set out in paragraphs 1, 2 or 3 of this Article shall be sentenced as if he himself/she herself has committed the crime.

Terrorism

Article 97

(1) Whoever, with a view to seriously intimidating a population or compelling a government or an international organisation to do or to abstain from doing an act or seriously destabilising or destroying the fundamental constitutional, political, economic or social structures of a state or an international organisation, commits any of the following acts which can seriously harm a state or an international organisation:

1. attacking a person's life which may cause death;

2. attacking the physical integrity of a person;

3. kidnapping or hostage taking;

4. causing destruction to a government or public facility, a transport system, an infrastructure facility, including an information system, a fixed platform located on the epicontinental shelf, a public place or private property, which is likely to endanger human life or result in major economic loss;

5. hijacking an aircraft, vessel or other means of public or goods transport;

6. manufacturing, possessing, acquiring, transporting, supplying or using weapons, explosives or nuclear, biological or chemical weapons as well as doing research into and developing nuclear, biological or chemical weapons;

7. releasing dangerous substances, or causing fires, explosions or floods, the effect of which is to endanger human life;

8. interfering with or disrupting the supply of water, power or any other fundamental natural resource, the effect of which is to endanger human life; or

9. possessing or using radioactive substances or manufacturing, possessing or using a device for the activation, dispersal or emission of radioactive material or ionising radiation, using or causing damage to a nuclear facility resulting in the release of radioactive materials or the danger

thereof, or requesting, by using force or threats, radioactive materials, a device for activating, dispersing or emitting radioactive materials or a nuclear facility

shall be sentenced to imprisonment for a term of between three and fifteen years.

(2) Whoever threatens to commit a criminal offence referred to in paragraph 1 of this Article

shall be sentenced to imprisonment for a term of between six months and five years.

(3) If extensive destruction or the death of one or more persons has been caused by the criminal offence referred to in paragraph 1 of this Article,

the perpetrator shall be sentenced to imprisonment for a term of at least five years.

(4) If, in the course of perpetrating the criminal offence referred to in paragraph 1 of this Article, the perpetrator intentionally kills one or more persons,

he/she shall be sentenced to imprisonment for a term of at least ten years or to long-term imprisonment.

Financing of Terrorism

Article 98

(1) Whoever directly or indirectly provides or collects funds with the intention that they be used or in the knowledge that they will be used, in full or in part, in order to carry out one or more of the criminal offences referred to in Article 97, Articles 99 through 101, Article 137, Article 216, paragraphs 1 through 3, Article 219, Article 223, Article 224, Articles 352 through 355 of this Act or any other criminal offence intended to cause death or serious bodily injury to a civilian or to any other person not taking an active part in an armed conflict, when the purpose of such an act is to intimidate a population or to compel a government or an international organisation to do or to abstain from doing an act

shall be sentenced to imprisonment for a term of between one and ten years.

(2) The sentence referred to in paragraph 1 of this Article shall be imposed on whoever directly or indirectly provides or collects funds with the intention that they be used or in the knowledge that they will be used, in full or in part, by terrorists or terrorist associations.

(3) The funds referred to in paragraphs 1 and 2 of this Article shall be confiscated.

Public Instigation of Terrorism

Article 99

Whoever publicly expresses or promotes ideas directly or indirectly instigating the commission of a criminal offence referred to in Articles 97 through 98, Article 137, Article 216, paragraphs 1 through 3, Article 219, Articles 223 through 224, Articles 352 through 355 of this Act

shall be sentenced to imprisonment for a term of between one and ten years.

Recruitment for Terrorism

Article 100

Whoever solicits another person to join a terrorist association for the purpose of contributing to the commission of a criminal offence referred to in Articles 97, 102, 137, Article 216, paragraphs 1 through 3, Articles 219, 223, 224, Articles 352 through 355 of this Act

shall be sentenced to imprisonment for a term of between one and ten years.

Training for Terrorism

Article 101

Whoever provides instructions in the making or use of explosive devices, firearms or other weapons or noxious or hazardous substances, or in other specific methods or techniques, knowing that the skills provided are intended to be used for the purpose of committing any of the

criminal offences referred to in Articles 97, 98, 137, Article 216, paragraphs 1 through 3, Article 219, Articles 223 through 224, Articles 352 through 355 of this Act

shall be sentenced to imprisonment for a term of between one and ten years.

Terrorist Association

Article 102

(1) Whoever organises or runs a criminal association the aim of which is to commit a criminal offence referred to in Articles 97 through 101, Article 137, Article 216, paragraphs 1 through 3, Article 219, Articles 223 through 224, Articles 352 through 355 of this Act or any other criminal offence intended to cause death or serious bodily injury to a civilian or to any other person not taking an active part in an armed conflict, when the purpose of such an act is to intimidate a population or to compel a government or an international organisation to do or to abstain from doing an act

shall be sentenced to imprisonment for a term of between three and fifteen years.

(2) Whoever becomes a member of the criminal association referred to in paragraph 1 of this Article or commits an act which he/she knows contributes to the achievement of the terrorist association's goal

shall be sentenced to imprisonment for a term of between one and eight years.

(3) The perpetrator of a criminal offence referred to in paragraph 1 or 2 of this Article who, by uncovering a terrorist association on time, prevents the perpetration of a criminal offence referred to in paragraph 1 of this Article or a member of a terrorist association who uncovers the association prior to committing, as its member or on its behalf, a criminal offence referred to in paragraph 1 of this Article may have his/her punishment remitted.

Abduction

Article 137

(1) Whoever unlawfully deprives another of liberty in order to force a third party to do or omit to do something or to suffer

shall be sentenced to imprisonment for a term of between six months and five years.

(2) If the criminal offence referred to in paragraph 1 of this Article was committed under threat that the abducted person would be killed or was committed in a cruel way or the abducted person suffered a severe bodily injury or the said criminal offence was committed against a child or a disabled person,

the perpetrator shall be sentenced to imprisonment for a term of between one and ten years.

(3) If the abducted person died as a result of the criminal offence referred to in paragraph 1 of this Article,

the perpetrator shall be sentenced to imprisonment for a term of between three and fifteen years.

(4) A perpetrator who of his/her free will releases an abducted person before he/she achieves the goal referred to in paragraphs 1 and 2 of this Article may be exempted from punishment.

Destruction of or Damage to Public-Use Devices

Article 216

(1) Whoever destroys, damages, modifies, renders unusable, removes, disconnects or disrupts the functioning of a public-use device for water, heat, gas, electricity or other energy or of electronic communications equipment and thus causes a disruption to the regular life of a population

shall be sentenced to imprisonment for a term of between six months and five years.

(2) The sentence referred to in paragraph 1 shall be imposed on whoever destroys, damages, disconnects, redirects or otherwise disrupts the proper working order of a subsea cable or pipeline which below sea level enables the provision of an electronic communications service or the flow of water, gas, oil or electricity between two or more countries or between a country and the Arctic or Antarctic.

(3) The sentence referred to in paragraph 1 of this Article shall be imposed on whoever destroys, damages or otherwise disrupts the proper working order of auxiliary facilities, vessels, devices or equipment that is used for installation, repair or maintenance of subsea cables or pipelines.

(4) Whoever commits the criminal offence referred to in paragraph 1, 2 or 3 of this Article by negligence

shall be sentenced to imprisonment for a term of up to three years.

Misuse of Radioactive Substances

Article 219

(1) Whoever with the aim of killing or inflicting a severe bodily injury on another person or of causing considerable damage to another person's property or the environment produces, processes, procures, possesses, stocks, transports, imports, exports, gives to another or enables another to acquire without authorisation radioactive substances or a device for activating, dispersing or emitting radioactive substances

shall be sentenced to imprisonment for a term of between six months and five years.

(2) The sentence referred to in paragraph 1 of this Article shall be imposed on whoever with the aim of killing or inflicting a severe bodily injury on another person or of causing considerable damage to another person's property or the environment uses radioactive substances or a device for activating, dispersing or emitting radioactive substances, or uses or damages a nuclear facility, thus causing the danger of radioactive substances being released.

(3) The sentence referred to in paragraph 1 of this Article shall be imposed on whoever by the use or threats of use of force demands without authorisation the handing over of a nuclear facility or of radioactive substances or of a device for activating, dispersing or emitting radioactive substances.

Endangering Traffic by a Dangerous Act or Dangerous Means

Article 224

(1) Whoever destroys, damages, removes or otherwise makes unusable or unnoticeable a sign or device ensuring the safety of rail, sea, inland water or air traffic

shall be sentenced to imprisonment for a term of up to one year.

(2) Whoever destroys, damages, removes or otherwise makes unusable or unnoticeable a sign, device or traffic mechanism ensuring the safety of any type of traffic, or erects obstructions, gives false information, signs or signals or otherwise endangers traffic and thus also the life or limb of people or property of considerable value

shall be sentenced to imprisonment for a term of between six months and five years.

(3) Whoever commits the criminal offence referred to in paragraph 2 of this Article by negligence

shall be sentenced to imprisonment for a term of up to three years.

(4) If as a result of the criminal offence referred to in paragraph 2 of this Article a person suffers an injury or considerable damage to property is caused,

the perpetrator shall be sentenced to imprisonment for a term of between one and ten years.

(5) If as a result of the criminal offence referred to in paragraph 2 of this Article one or more persons die,

the perpetrator shall be sentenced to imprisonment for a term of between three and fifteen years.

(6) If as a result of the criminal offence referred to in paragraph 3 of this Article a person suffers a severe bodily injury or considerable damage to property is caused,

the perpetrator shall be sentenced to imprisonment for a term of between one and eight years.

(7) If as a result of the criminal offence referred to in paragraph 3 of this Article one or more persons die,

the perpetrator shall be sentenced to imprisonment for a term of between one and ten years.

Money Laundering

Article 265

(1) Whoever invests, takes over, converts, transfers or replaces a pecuniary advantage derived from criminal activity for the purpose of concealing or disguising its illicit origin

shall be sentenced to imprisonment for a term of between six months and five years.

(2) The sentence referred to in paragraph 1 of this Article shall be imposed on whoever conceals or disguises the true nature, source , location, disposition, movement, rights with respect to, or ownership of a pecuniary advantage derived by another from criminal activity.

(3) The sentence referred to in paragraph 1 of this Article shall be imposed on whoever acquires, possesses or uses the pecuniary advantage derived by another from criminal activity.

(4) Whoever commits the offence referred to in paragraph 1 or 2 of this Article in financial or other dealings or where the perpetrator engages professionally in money laundering or the pecuniary advantage referred to in paragraph 1, 2 or 3 of this Article is of considerable value,

shall be sentenced to imprisonment for a term of between one and eight years.

(5) Whoever commits the offence referred to in paragraph 1, 2 or 4 of this Article through negligence with respect to the circumstance that the pecuniary advantage is derived from criminal activity

shall be sentenced to imprisonment for a term of up to three years.

(6) If the pecuniary advantage referred to in paragraphs 1 through 5 of this Article is derived from criminal activity carried out in a foreign country, the perpetrator shall be punished when the activity is a criminal offence also under the domestic law of the country where it is committed.

(7) The perpetrator referred to in paragraphs 1 through 5 of this Article who contributes of his/her own free will to the discovery of the criminal activity from which a pecuniary advantage has been derived may have his/her punishment remitted.

Unlawful Release of a Person Deprived of Liberty

Article 299

A public official who unlawfully releases a person deprived of liberty or assists him/her in his/her escape

shall be sentenced to imprisonment for a term of between one and eight years.

Aiding the Perpetrator Following the Commission of a Criminal Offence

Article 303

(1) Whoever conceals or harbours the perpetrator of a criminal offence for which a sentence of imprisonment of five years or a more severe sentence is prescribed, or by concealing the means by which the criminal offence was committed, traces of the criminal offence or objects which are the product of or which were obtained by the criminal offence or otherwise aids him/her in avoiding detection or apprehension

shall be sentenced to imprisonment for a term of between six months and five years.

(2) The sentence referred to in paragraph 1 of this Article shall be imposed on whoever conceals a person sentenced to imprisonment or otherwise prevents the execution of this sentence.

(3) Whoever commits the criminal offence referred to in paragraph 1 or 2 of this Article to the benefit of the perpetrator of any of the criminal offences referred to in Articles 88 through 91 or Article 97 of this Act

shall be sentenced to imprisonment for a term of between one and eight years.

(4) The perpetrator of the criminal offence referred to in paragraph 2 of this Article shall not be imposed a punishment more severe than the one prescribed for the criminal offence committed by the person to whom the perpetrator provided assistance.

(5) There shall be no criminal offence referred to in paragraphs 1, 2 and 3 of this Article where its statutory elements are realised by a person who is married to, or lives in a cohabiting or same-sex relationship with, or is a lineal blood relative, sibling, adopter or adoptee of the person to whom he/she provided assistance.

Conspiracy to Commit a Criminal Offence

Article 327

(1) Whoever conspires with another to commit a criminal offence for which a sentence of imprisonment for a term exceeding three years may be imposed under the law

shall be sentenced to imprisonment for a term of up to three years.

(2) A perpetrator who uncovers the conspiracy referred to in paragraph 1 of this Article before the agreed upon criminal offence is committed may have his/her punishment remitted.

Criminal Association

Article 328

(1) Whoever organises or directs a criminal association

shall be sentenced to imprisonment for a term of between six months and five years.

(2) Whoever participates in the association referred to in paragraph 1 of this Article but has not as yet committed any criminal offence for this association, or whoever carries out an act which in itself does not constitute a criminal offence but which he/she knows furthers the goal of a criminal association, or whoever financially or otherwise abets a criminal association

shall be sentenced to imprisonment for a term of up to three years.

(3) The perpetrator of a criminal offence referred to in paragraph 1 or 2 of this Article who by timely disclosure of a criminal association prevents the commission of any of the criminal offences set forth in paragraph 4 of this Article or a member of a criminal association who discloses a criminal association before committing, as its member or on its behalf, any of the criminal offences set forth in paragraph 4 of this Article may have his/her punishment remitted.

(4) A criminal association shall be made up of three or more persons acting in concert with the aim of committing one or more criminal offences that are punishable with imprisonment for a term longer than three years and shall not include an association randomly formed for the immediate commission of one criminal offence.

Committing a Criminal Offence as a Member of a Criminal Association

Article 329

(1) Whoever, knowing about the goal of a criminal association or its criminal activities, commits a criminal offence as a member of such an association or incites another to commit a criminal offence as a member of such an association shall be sentenced:

1. to imprisonment for a term of between six months and five years in the case of a criminal offence for which a maximum penalty of three years is prescribed;
2. to imprisonment for a term of between one and ten years in the case of a criminal offence for which a maximum penalty of five years is prescribed;
3. to imprisonment for a term of between three and twelve years in the case of a criminal offence for which a maximum penalty of eight years is prescribed;
4. to imprisonment for a term of between three and fifteen years in the case of a criminal offence for which a maximum penalty of ten or twelve years is prescribed;
5. to imprisonment for a term of between five and twenty years in the case of a criminal offence for which a maximum penalty of fifteen years is prescribed;
6. to imprisonment for a term of at least ten years or to long-term imprisonment in the case of a criminal offence for which a maximum penalty of twenty years is prescribed.

(2) Whoever, knowing about the goal of a criminal association or its criminal activity, aids or abets another to commit a criminal offence as a member of such an association shall be imposed a sentence prescribed in paragraph 1 of this Article or may incur a less severe sentence.
(3) If the perpetrator referred to in paragraph 1 or 2 of this Article substantially contributes to the discovery of a criminal association, he/she may incur a less severe sentence.

Murder of an Internationally Protected Person

Article 352

(1) Whoever kills an internationally protected person

shall be sentenced to imprisonment for a term of at least ten years or to long-term imprisonment.

(2) An internationally protected person shall mean a head of state, head of Government or minister for foreign affairs, whenever any such person is in a foreign state, and any official agent of an internationally recognised organisation, as well as members of their families accompanying them when they, their official premises, private accommodation or means of transport can easily be recognised as enjoying special protection under international law.

Kidnapping of an Internationally Protected Person

Article 353

(1) Whoever kidnaps an internationally protected person

shall be sentenced to imprisonment for a term of between three and twelve years.

(2) If by the commission of the criminal offence referred to in paragraph 1 of this Article the death of the kidnapped person is caused,

the perpetrator shall be sentenced to imprisonment for a term of at least five years.

Attack on an Internationally Protected Person

Article 354

(1) Whoever commits violence against an internationally protected person or attacks his/her official premises, private accommodation or means of transport

shall be sentenced to imprisonment for a term of between one and eight years.

(2) If by the commission of the criminal offence referred to in paragraph 1 of this Article the death of the person referred to in paragraph 1 of this Article is caused,

the perpetrator shall be sentenced to imprisonment for a term of between three and twelve years.

Threat to an Internationally Protected Person

Article 355

Whoever jeopardises the safety of an internationally protected person by a serious threat of committing against the said person any of the criminal offences referred to in Articles 352 through 354 of this Act shall be sentenced to imprisonment for a term of between six months and five years.

ANNEX IV Criminal Code 2004

Applicability of Criminal Legislation to Criminal Offences Committed Outside the Territory of the Republic of Croatia

Article 14

(1) The criminal legislation of the Republic of Croatia shall apply to anyone who, outside its territory, commits:
– any criminal offence against the Republic of Croatia provided for in Chapter (xii) of this Code;
– the criminal offence of counterfeiting money and securities of the Republic of Croatia as defined in Articles 274 and 275 of this Code;
– a criminal offence which the Republic of Croatia is bound to punish according to the provisions of international law and international treaties or intergovernmental agreements;
– a criminal offence against a Croatian state official or a civil servant relating to his office.

(2) The criminal legislation of the Republic of Croatia shall be applied to a Croatian citizen who, outside the territory of the Republic of Croatia, commits a criminal offence other than those specified in paragraph 1 of this Article.

(3) The criminal legislation of the Republic of Croatia shall be applied to an alien who, outside the territory of the Republic of Croatia, commits a criminal offence against the Republic of Croatia or its citizens which is not specified in paragraph 1 of this Article.

(4) The criminal legislation of the Republic of Croatia shall be applied to an alien who, outside the territory of the Republic of Croatia, commits against a foreign state or another alien a criminal offence for which, under the law in force in the place of crime, a punishment of five years of imprisonment or a more severe penalty may be applied.

(5) In the cases referred to in paragraphs 2 and 3 of this article, the criminal legislation of the Republic of Croatia shall be applied only if the perpetrator of the criminal offence is found within the territory of the Republic of Croatia, or has been extradited to it, and in the case referred to in paragraph 4 of this Article, only if the perpetrator is found within the territory of the Republic of Croatia and is not extradited to another state.

Particularities Regarding the Institution of Criminal proceedings for Criminal Offences Committed outside the Territory of the Republic of Croatia

Article 16

(1) In the cases specified in article 14, paragraphs 2, 3 and 4 of this Code, criminal proceedings for the purpose of applying the criminal legislation of the Republic of Croatia shall not be instituted:

– if the perpetrator has served in full the sentence imposed on him in a foreign state;
- if the perpetrator has been acquitted by a final judgement in a foreign state, or if he has been pardoned, or if the statutory time limitation has expired under the law in force in the country of the perpetration;
- if, under the law in force in the country of the perpetration, criminal proceedings may be instituted only upon a motion, a consent or a private charge of the person against whom the criminal offence had been committed, and such a motion was not made or a private charge was not brought, or the consent was not given.

(2) If, in the cases specified in Article 14, paragraphs 2, 3 and 4 of this Code, such an act does not constitute a criminal offence under the law in force in the country of the perpetration, criminal proceedings may be constituted only upon the approval of the State Attorney of the Republic of Croatia.

(3) In the case referred to in Article 14, paragraph 4 of this Code, when the committed act is not punishable under the law in force in the country in which it was committed but is deemed to be a criminal offence according to the general principles of law of the international community, the State Attorney of the Republic of Croatia may authorize the institution of criminal proceedings in the Republic of Croatia and the application of the criminal legislation of the Republic of Croatia.

Aiding and Abetting

Article 38

(1) Whoever intentionally aids and abets another in the perpetration of a criminal offence shall be punished as if he himself committed it, but the punishment may also be mitigated.

(2) The following shall in particular be deemed acts of aiding and abetting: giving advice or instructions on how to commit a criminal offence, providing the perpetrator with the means for the perpetration of a criminal offence, removing obstacles for the perpetration of a criminal offence, giving an advance promise to conceal the criminal offence, the perpetrator, or the means by which the criminal offence was committed, as well as concealing the traces of a criminal offence or the objects procured by the criminal offence.

International Terrorism

Article 169

(1) Whoever aims to cause major fear among the population, to force foreign states or international organizations to do or not do something or suffer, or who aims to seriously jeopardize the fundamental constitutional, political or economic values of a foreign state or an international organization, who commits a criminal offence referred to in Articles 170 through 172, and Articles 179 and 181 of this Code, who causes an explosion or fire, or by a generally perilous act or means creates a dangerous situation for people or property, who kidnaps a person or commits another violent act which can seriously harm a foreign state or an international organization

shall be punished by imprisonment for not less than three years.

(2) Whoever seriously threatens to commit a criminal offence referred to in paragraph 1 of this Article

shall be punished by imprisonment for one to five years.

(3) If, by the criminal offence referred to in paragraph 1 of this Article, the death of one or more persons is caused,

the perpetrator shall be punished by imprisonment for not less than ten years or by long-term imprisonment.

(4) If, by the criminal offence referred to in paragraph 1 of this Article, the death of one or more persons or large-scale destruction is caused,

the perpetrator shall be punished by imprisonment for not less than five years.

(5) In order to initiate criminal proceedings for the criminal offence referred to in this Article, an approval from the State Attorney of the Republic of Croatia is required.

Planning Criminal Offences against Values Protected by International law

Article 187a

(1) Whoever removes obstacles, makes a plan or arrangements with others or undertakes any other action to create the conditions for the direct perpetration of criminal offences referred to in Articles 156 through 160, Articles 169 through 172, and Articles 179 and 181 of this Code

shall be punished by imprisonment for one to five years.

(2) The same punishment as referred to in paragraph 1 of this Article shall be inflicted on whoever procures or collects financial means, being aware that they shall be used in total or partially for the perpetration of the criminal offences referred to in the para 1 of this Article.

Money Laundering

Article 279

(1) Whoever, in banking, financial or other economic operations, invests, takes over, exchanges or otherwise conceals the true source of money, objects or rights procured by money which he knows to be acquired by a criminal offence

shall be punished by imprisonment for six months to five years.

(2) The same punishment as referred to in paragraph 1 of this Article shall be inflicted on whoever acquires, possesses or brings into circulation for himself or for another the money, objects or rights referred to in paragraph 1 of this Article, although at the moment of acquisition he knew the origin of such.

(3) Whoever commits the criminal offence referred to in paragraphs 1 and 2 of this Article as a member of a group or a criminal organization

shall be punished by imprisonment for one to ten years.

(4) Whoever, committing the criminal offence referred to in paragraphs 1 and 2 of this Article, acts negligently regarding the fact that the money, objects or rights are acquired by the criminal offence referred to in paragraph 1 of this Article

shall be punished by imprisonment for three months to three years.

(5) If the money, objects or rights referred to in paragraphs 1, 2 and 4 of this Article are acquired by a criminal offence committed in a foreign state, such an offence shall be evaluated pursuant to the provisions of the Croatian criminal legislation taking into consideration the provisions of Article 16, paragraphs 2 and 3 of this Code.

(6) The money and objects referred to in paragraphs 1, 2 and 4 of this Article shall be forfeited while the rights referred to in paragraphs 1, 2 and 4 shall be pronounced void.

(7) The court may remit the punishment of the perpetrator of the criminal offence referred to in paragraphs 1, 2, 3 and 4 of this Article who voluntarily contributes to the discovery of such a criminal offence.

ANNEX V Criminal Procedure Code 2009

Article 206

(1) After inspection of the report and verification in the Information System of the State Attorney, the State Attorney shall dismiss a crime report by a ruling with a statement of reasons:

1) if it follows from the report that the reported act is not a criminal offence subject to public prosecution;
2) if the period of limitation for the institution of prosecution has expired and if the offence is amnestied or pardoned,
3) if other circumstances exist excluding culpability or barring prosecution,
4) if no reasonable suspicion exists that the suspect committed the reported offence,
5) if the data in the report point to the conclusion that the report is not credible.

(2) The ruling of the State Attorney on the dismissal of the crime report shall not be subject to appellate review.

(3) Unless otherwise stipulated by this Act (Article 521 and 522), the State Attorney shall notify the injured person within eight days on the dismissal of the report and on the grounds thereof except if he decides not to institute prosecution in cases from Article 212 of this Act, with the instruction from Article 55 of this Act, and if the report was made by the police authorities or another state authority, the State Attorney shall notify the person who filed a crime report and upon his request the person against which the report was made.

(4) If the State Attorney is unable to establish from the crime report whether or not allegations in the report are credible, or if facts stated in the report do not suffice for a decision on whether he should order the opening of an investigation, or undertake evidence collecting actions, or if only rumors reach the State Attorney that a criminal offence has been committed, the State Attorney shall, if he cannot do this himself or through other authorities, order the police authorities to obtain necessary information by making inquiries and undertaking other measures for collecting the data necessary for a decision on the opening of the investigation. The State Attorney may in his order to the police authorities determine the content of the inquiry or measure in more detail and order immediate information from the police authorities about the inquiry or measure undertaken. If the State Attorney orders to be present during the inquiry or measure, the police authorities shall undertake the inquiry or measure in such a manner as to enable his presence. The police authorities are bound to proceed in accordance with the order of the State Attorney, and unless the State Attorney has ordered otherwise, they shall notify the State Attorney within a term of thirty days from the submission of the request of the inquiries or measures undertaken.

(5) Upon the request of the State Attorney, the police authorities, the ministry responsible for finance, the State Audit Office and other state authorities, organizations, bank and other legal entities shall deliver to the State Attorney required information, except the information representing a lawfully protected secret. The State Attorney may request from the aforesaid authorities to control the operations of a legal entity or physical person and, according to the appropriate regulations, to seize temporarily, until a judgement is rendered, of money, valuable securities, objects and documentation that may serve as evidence, to perform supervision and delivery of data that may serve as evidence on the committed criminal offence or property gained by the criminal offence, and to request information on collected, processed and stored data regarding unusual and suspicious monetary transactions. In his request, the State Attorney may in more detail specify the content of the requested measure or action and demand to be informed thereof, in order to be able to attend its execution.

(6) For failure to comply with the request, the investigating judge may, upon a motion with the statement of reasons by the State Attorney, impose a fine to the responsible person in the amount of up to HRK 50,000.00, and to legal entity in the amount of up to HRK 5,000,000.00, and if even after that such person fails to act upon the request, the person may be punished with imprisonment until the request is complied with, and not longer than one month. The court which rendered the ruling on imprisonment may abolish the ruling if, after the ruling was rendered, the responsible person acts according to the request.

(7) The State Attorney may for the purpose of collecting necessary information summon the person who filed a crime report and other persons if he considers that their statements may contribute to the

assessment of the credibility of the allegations made in the report. The summons shall state the reasons for the summons. If the person who is summoned fails to answer, it shall be preceded according to Article 208 paragraph 3 of this Act.
(8) If the crime report does not contain the data on the criminal offence or if the State
Attorney cannot conclude from the crime report for which criminal offence the report is filed, the person who filed a crime report shall be summoned to correct and supplement the crime report within fifteen days. If the person who filed a crime report fails to act on the summons to correct or supplement the report, the State Attorney shall make a note thereof and attach the crime report and the summons for correction or supplement thereto. Such crime report shall not be entered recorded in the crime report register; instead it shall be entered in the register of miscellaneous criminal files. The crime report and the summons shall be stored. The higher State Attorney shall be notified thereof within seven days from the expiry of the period for correction or supplement of the crime report, who may order entering of the crime report in the crime report register.
(9) The State Attorney shall make the records on the collected statement as referred to in paragraph 7 of this Article which, as well as the material referred to in Article 208 paragraph 5 of this Act, may be used during the evidence collecting actions before preferring the indictment. The records and material shall be excluded from the file pursuant to Article 86 paragraph 3 of this Act and may not be used as evidence in the proceedings.
(10) The minister responsible for justice shall regulate the method for keeping the register referred to in paragraph 8 of this Article.

2. Temporary Seizure of Objects

Article 261

(1) Objects which have to be seized pursuant to the Penal Code or which may be used to determine facts in proceedings shall be temporarily seized and deposited for safekeeping.
(2) Whoever is in possession of such objects shall be bound to surrender them upon the request of the State Attorney, the investigator or the police authorities. The State Attorney, the investigator or the police authorities shall instruct the holder of the object on consequences arising from denial to comply with the request.
(3) A person who fails to comply with the request to surrender the objects, even though there are no justified causes, may be penalized by the investigating judge upon a motion with a statement of reasons of the State Attorney pursuant to Article 259 paragraph 1 of this Act.
(4) The measures referred to in paragraph 2 of this Article shall not apply either to the defendant or persons who are exempted from the duty to testify (Article 285).

Article 262

(1) Temporary seizure shall not apply to:
1) files and other documents of state authorities, the publication of which would violate the confidentiality obligation, until decided otherwise by the competent authority;
2) written notices of the defendant to the defence counsel, unless the defendant requires otherwise;
3) tapes and private diaries found with the persons referred to in Article 285 paragraphs 1 to 3 of this Act, which were taken or written by this person and contain recordings or notes on the facts regarding which these persons are exempted from the duty to testify;
4) records, registry excerpts and similar documents possessed by the persons referred to in Article 285 paragraph 1 item 3 of this Act that have been made by these persons regarding facts disclosed to them by the defendant while performing their respective professions;
5) written records of facts made by journalists and editors in the media regarding sources of information and data disclosed to them during performance of their profession and which were used in the media editorial process and which are in their possession or in possession of the editorial office they work for;
(2) The ban on the temporary seizure of objects, documents and recordings referred to paragraph 1 items 2 to 5 of this Article shall not apply:

1) with regard to a defence counsel or persons who are exempted from the duty to testify pursuant to Article 285 paragraph 1 of this Act if there is probability that they have helped the defendant in committing the criminal offence, assisted him after committing the criminal offence or acted as accessories;
2) with regard to journalists and editors in the media if there is probability that they have helped the defendant in committing the criminal offence, assisted him after committing the criminal offence or acted as accessories of the criminal offence, and criminal offences referred to in Article 305 and 305(a) of the Penal Code;
3) in case these are objects that may be seized pursuant to law;
(3) Until preferring the indictment, at the request of the State Attorney, the investigating judge shall decide by a ruling on the probability of providing help in the criminal offence referred to in paragraph 2 of this Article. The investigating judge shall bring a ruling within 24 hours from the submission of the request by the State Attorney. The panel shall decide on the appeal against the ruling of the investigating judge. After preferring the indictment, the court before which the proceeding is conducted shall bring a decision. The appeal against the decision of the indictment panel and the trial court shall not be allowed.
(4) The ban on temporary seizure of objects, documents and recordings pursuant to paragraphs 1, items 2 and 3 of this Article shall not apply in relation to investigations of criminal offence committed against children and minors referred to in Article 117 of the Juvenile Court Act.
(5) The State Attorney, the investigator or the police authorities may seize objects pursuant to paragraphs 1, 2 and 3 of this Article even when they are carrying out inquiries into criminal offences or when the investigator or the police authorities are executing a court's warrant.
(6) When seizing an object it shall be noted in the record where it has been found and it shall be described, and if necessary its identity shall be stipulated in another way. A receipt shall be issued for temporarily seized objects.
(7) An object seized contrary to the provisions of paragraph 1 of this Article cannot be used as evidence in criminal proceedings.

Article 263

(1) The provisions of Article 261 of this Act also apply to data saved on the computer and devices connected thereto, as well as on devices used for collecting and transferring of data, data carriers and subscription information that are in possession of the service provider, except in case when temporary seizure is prohibited pursuant to Article 262 of this Act.
(2) Data referred to in paragraph 1 of this Act must be handed over to the State Attorney upon his written request in an integral, original, legible and understandable format. The State Attorney shall stipulate a term for handing over of such data in his request. In case handing over is denied, it may be pursued in accordance with Article 259 paragraph 1 of this Act.
(3) Data referred to in paragraph 1 of this Act shall be recorded in real time by the authority carrying out the action. Attention shall be paid to regulations regarding the
obligation to observe confidentiality (Articles 186 to 188) during acquiring, recording, protecting and storing of data. In accordance with the circumstances, data not related to the criminal offence for which the action is taken, and are required by the person against which the measure is applied, may be recorded to appropriate device and be returned to this person even prior to the conclusion of the proceedings.
(4) Upon a motion of the State Attorney, the investigating judge may by a ruling decide on the protection and safekeeping of all electronic data from paragraph 1 of this Article, as long as necessary and six months at longest. After this term data shall be returned, unless:
1) they are related to committing the following criminal offences referred to in the Penal Code: breach of confidentiality, integrity and availability of electronic data, programs and systems (Article 223), computer forgery (Article 223a) and computer fraud (Article 224a);
2) they are related to committing another criminal offence which is subject to public prosecution, committed by using a computer system;
3) they are not used as evidence of a criminal offence for which proceedings are instituted.

(5) The user of the computer and the service provider may file an appeal within twenty-four hours against the ruling of the investigating judge prescribing the measures referred to in paragraph 3 of this Article. The panel shall decide on the appeal within three days. The appeal shall not stay the execution of the ruling.

Article 264

(1) State authorities may refuse to present or surrender their files and other documents if these are confidential information pursuant to a special law (classified information).
(2) Legal entities may request that data related to their business be not disclosed.
(3) A decision on declassification of data pursuant to paragraph 1 of this Article shall be made by the state authority upon the motion of the State Attorney or the court.
(4) A decision on disclosure of data referred to in paragraph 2 of this Article shall be made by the investigating judge or the court before which the hearing is conducted upon the motion with a statement of reasons of the State Attorney. The ruling of the court before which the hearing is conducted shall not be subject to appellate review.

Article 265

(1) If access to data considered to be a bank secret is denied, the court may issue a ruling on disclosure of data representing a bank secret upon the motion with a statement of reasons of the State Attorney. The court shall stipulate the term within which the bank must disclose data in the ruling.
(2) When it is probable that a certain person receives, holds or disposes in any other way of income arising from a criminal offence on his bank account and this income is important for the investigation of that criminal offence or it underlies forceful seizure, the State Attorney shall, by a request with a statement of reasons, propose to the court to order the bank to hand over data on that account and income to the State Attorney. The request shall include data on legal entity or physical person who holds these means or this income or disposes of them. A description of income must include the currency designation, but not its exact amount if it is not known. The court shall stipulate a term within which the bank must proceed as ordered.
(3) Before the commencement and during the investigation a decision on the request of the State Attorney referred to in paragraph 1 and 2 of this Article shall be brought by the investigating judge, on indictment by the panel examining the indictment, and after it becomes final by the court before which the hearing is to be conducted.
(4) The investigating judge shall decide on the State Attorney's request referred to in paragraphs 1 and 2 of this Article immediately or within twelve hours at the latest from the receipt of the request. Should the investigating judge deny the request, the State Attorney may file an appeal within twelve hours. The panel shall decide on the appeal within twenty-four hours. An appeal against the ruling of the court brought on indictment shall not be allowed.
(5) If circumstances referred to paragraphs 2 and 3 of this Article exist, the investigating judge may upon the motion with a statement of reasons of the State Attorney order the bank or any other legal entity to follow up on money transfer and transactions on the account of a certain person and to regularly inform the State Attorney thereof during the term stipulated in the ruling.
(6) Measures of the follow-up on money transfer may be applied for a year at longest.
As soon as the reasons for the follow-up have ceased to exist, the State Attorney shall inform the investigating judge who shall cancel the follow-up by a ruling. Should the State Attorney desist from the criminal prosecution or the evidence collected are not required for the criminal proceedings, data on the follow-up shall be destroyed under supervision of the investigating judge who shall compile a special record thereon. The State Attorney shall deliver the ruling on the follow-up to the person against whom it was issued, together with the indictment or the decision on desisting from the criminal prosecution.
(7) The bank or any other legal entity shall refrain from disclosure of information or data on the proceedings pursuant to paragraphs 1 to 5 of this Article.
(8) Upon the motion with a statement of reasons of the State Attorney, the investigating judge shall by a ruling impose a fine amounting to HRK 1,000,000.00 upon the bank and a fine amounting to HRK

200,000.00 upon the responsible person in the bank or any other legal person for proceedings contrary to paragraphs 1 to 5 of this Article. In case the order is not complied with even after such a fine, the responsible person may be punished by imprisonment until the order is executed, but not longer than one month. The appeal against the ruling on a fine and imprisonment shall not stay the execution of the ruling.

Article 266

(1) Upon the motion with a statement of reasons of the State Attorney, the court may order by a ruling a legal entity or a physical person to suspend temporarily the execution of a financial transaction if the suspicion exists that it represents an offence or that it serves to conceal an offence or to conceal the benefit obtained in consequence of the commission of an offence.
(2) By the ruling referred to in paragraph 1 of this Article the court shall order that the financial means assigned for the transaction referred to in paragraph 1 of this Article and cash amounts of domestic and foreign currency temporarily seized pursuant to Article 256 paragraph 2 of this Act shall be deposited in a special account and be kept safe until the termination of the proceedings, or until the conditions are met for their recovery, but not longer than two years. After the indictment becomes final, the court may prolong the duration of safekeeping to two years at longest.
(3) Before the commencement and during the investigation, the decision shall be made by the investigating judge, on indictment by the panel examining the indictment, and after it becomes final by the court before which the hearing is to be conducted. The investigating judge shall decide by a ruling on the State Attorney's request within twenty-four hours from the receipt of the request. Should the judge deny the request, the State Attorney may file an appeal within twelve hours. The panel shall decided on the appeal within twenty-four hours. The appeal shall not stay the execution of the ruling.
(4) A legal entity or a physical person must not reveal information or data on the proceeding pursuant to paragraphs 1 to 3 of this Article.

Article 267

(1) Files or documents which are temporarily seized because they may be used as evidence shall be listed. If this is not possible, files or documents shall be put in a separate cover and sealed. The person from whom a file or document is temporarily seized may put his own seal on the cover.
(2) The cover shall be opened by the State Attorney. While examining the file or document, attention must be paid not to disclose their contents to unauthorized persons. A record on the opening of the cover shall be made.
(3) The person from whom the files or documents have been seized shall be summoned to attend the opening of the cover. If this person fails to attend the opening or is absent, the cover shall be opened; the files or documents examined and a list of them made in his absence.

Article 268

In case of non compliance with the ruling of the court referred to in Article 265 paragraphs 1 to 5 and Article 266 paragraphs 1 to 3 of this Act or acting contrary to Article 265 paragraph 7 and Article 266 paragraph 4 of this Act, the legal entity shall be imposed a fine amounting up to HRK 1,000,000.00 and a responsible person of the legal entity or a physical person a fine amounting to HRK 200,000.00, and in case the decision is not executed even after that, a responsible or physical person may be punished by imprisonment until the decision is executed, but not longer than one month. The panel shall decide on the complaint against the ruling on a fine or imprisonment. The appeal against the ruling on a fine or imprisonment shall not stay the execution of the ruling. The punishment shall not interfere with the criminal prosecution for a criminal offence of disclosure of confidential data.

Article 269

(1) Objects that are to be used as evidence shall be kept in a special State Attorney's premise before preferring the indictment, and in a special court room after preferring the indictment. By way of

derogation, if that is not possible, the objects shall be kept outside the State Attorney's or the court's premises.
(2) The authority conducting the proceedings shall take care of supervision over these objects.
(3) The minister responsible for justice shall bring regulations to determine the method and conditions under which the objects referred to in paragraph 2 of this Article are kept.

Article 270

(1) Temporarily seized objects must be returned unless they underlay the provisions on seizing pursuant to law or if legal grounds for applying the measure referred to in Article 266 paragraph 2 of this Act cease to exist.
(2) The State Attorney and the court shall by virtue of the office pay attention to the existence of grounds for keeping temporarily seized objects.

Article 271

(1) Upon the motion of the State Attorney, temporary safety measures for the confiscation of pecuniary benefit may be ordered in the criminal proceedings pursuant to the provisions on the distraint procedure.
(2) The investigating judge shall decide on temporary safety measures until preferring the indictment, the panel examining the indictment upon preferring the indictment, and the trial court after that. The panel shall decide on the appeal against the decision of the investigating judge. The appeal against the decision by the panel examining the indictment and by the trial court shall not be allowed.
(3) A claim for indemnification for an ungrounded temporary measure shall be asserted in a civil action.

Article 455

(1) The court shall pronounce the judgement by which the accused is found guilty if it has been undoubtedly established that the accused committed the offence he has been charged with.
(2) In a judgement of conviction the court shall state:

1) the act for which the accused is found guilty, stating the facts and circumstance which constitute the elements of the definition of the offence as well as those on which the application of certain provisions of the Penal Code depends;
2) the legal name and description of the offence as well as the provisions of the Penal which were applied;
3) the punishment the accused is sentenced to or whether the punishment is remitted according to the provisions of the Penal Code, or whether the punishment of imprisonment is replaced with community service work;
3) the decision on a suspended sentence;
4) the decision on security measures and the confiscation of pecuniary benefit;
5) the decision on including the time spent in detention or served under an earlier sentence;
6) the decision on the costs of the proceedings, on the claim for indemnification and on the publication of the final judgement in the media.

(3) If the accused is sentenced to a fine, the judgement shall state the term within which the fine is to be paid as well as the amount of the daily income and the total number of daily incomes and the fine amount determined to a legal person.
(4) In case of concurrence of offences the court shall include, in the ordering part of the judgement, the punishments determined for each offence and thereafter the cumulative sentence rendered for all concurrent offences.

ANNEX VI Act on Proceedings for the Confiscation of the Pecuniary Benefits (Act on Confiscation)

I INTRODUCTORY PROVISIONS

Article 1

(1) This Act shall regulate:

a) the procedure of establishing pecuniary benefit resulting from criminal offences,
b) the procedure of confiscating pecuniary benefit resulting from criminal offences,
c) the enforcement procedure of a decision on the confiscation of pecuniary benefit resulting from criminal offences,
d) criminal proceedings regarding confiscated assets and the assets with respect to which a temporary measure has been imposed,
e) exercise of the rights of the person injured by the criminal offence, and
f) protection of rights of third parties.

(2) Provisions of other acts regulating the establishment, ensuring confiscation and enforcement of decisions on the confiscation of pecuniary benefits resulting from criminal offences and misdemeanours shall apply only unless otherwise prescribed by this Act.

(3) The court and the bodies which take actions in accordance with this Act, shall take into consideration whether the injured person has laid down property claims. If the injured person has laid down property claims which, with respect to their basis, exclude the confiscation of pecuniary benefit, actions to be taken pursuant to this Act shall only encompass the part of the pecuniary benefit resulting from criminal offences not included in the property claim.

(4) Actions pursuant to this Act shall be taken based on the proposal of the plaintiff.

(5) If establishing the value of pecuniary benefit resulting from criminal offences is linked to disproportionate difficulties or significant procrastination of criminal proceedings, the court may establish the value of the respective benefit at its own discretion.

(6) Unless otherwise prescribed by this Act, provisions of this Act shall apply to misdemeanour proceedings in the corresponding manner.

(7) Ex officio decisions in criminal proceedings pursuant to this Act shall be immediately delivered to the state attorney.

Article 2

(1) Proceedings pursuant to this Act may be conducted before, during or following the conclusion of criminal proceedings. Unless otherwise prescribed by this Act, the court shall take actions in accordance with criminal proceedings rules.

(2) If criminal proceedings can not be initiated for a criminal offence, because the defendant has died or other circumstances exist which exclude the possibility of criminal prosecution, upon proposal by the state attorney, the injured person as plaintiff or a private plaintiff, the court shall take actions in accordance with Article 6 of this Act, if the probable value of the pecuniary benefit resulting from criminal offences, with respect to which the actions are taken, is at least HRK 5,000.00.

(3) The decision to initiate criminal proceedings as described in paragraph 2 herein shall be reached in a ruling by a single judge from the court which would be competent for the trial in a criminal proceedings. An appeal may be filed against this decision within three days from the date the decision was delivered to the counterparty. A single judge from a court of the higher instance shall decide on the appeal.

(4) In the explanation of the ruling from paragraph 3 herein, the court shall set forth in particular the reasons for which no criminal proceedings may be conducted against the defendant.

(5) In criminal proceedings pursuant to this Act, the defendant and their related person shall have the status of a party.

(6) Provisions from paragraphs 2 - 4 of this Article shall not apply in misdemeanour proceedings.

II THE MEANING OF SPECIFIC EXPRESSIONS

Article 3

Specific expressions from this Act shall have the following meaning:

1. Pecuniary benefit resulting from criminal offences, pursuant to this and other Acts, refers to each increase or prevention of the reduction of property resulting from criminal offences;

2. Property represent assets and rights acquired by the perpetrator of a criminal offence and misdemeanour or their related party, and it refers to all property and rights which can be the object of enforcement, especially real estate and movables, claims, business interests, shares, money, precious metals and jewels in the ownership, possession or under the control of the criminal perpetrator or their related party;

3. A criminal offence is an act as prescribed by the Criminal Code;

4. A defendant is a physical and legal entity as prescribed by the Criminal Procedure Act and the Act on the Liability of Legal Entities for Criminal Acts;

5. An injured person is a physical and legal entity as prescribed by the Criminal Procedure Act;

6. A related party is:

a) a person who encourages and assists in the perpetration of the criminal offence,

b) a legal successor of the perpetrator and participant in the criminal offence and

c) another physical or legal entity, whom the court determined, as prescribed by this Act, to have been transferred property or rights representing pecuniary benefit and not to be in good faith related to such acquisition of the respective property or rights;

7. The plaintiff is a state attorney or other competent plaintiff, unless otherwise prescribed by this Act;

8. A counterparty is the defendant and their related person;

9. An opposing party and enforcement debtor is the defendant and their related person;

10. The proponent to ensure and bailiff is the plaintiff;

11. A third person is a person claiming, in regards to property which is the subject of criminal proceedings in accordance with this Act, to have rights preventing its application and requesting that the insurance or enforcement be pronounced illicit;

12. The Office is the Central Office for State Property Management or another body appointed by law for the management of state property.

(2) The terms from paragraph 1 of this Article shall also apply to misdemeanour proceedings in the corresponding manner.

III COURT PROCEEDINGS

Article 4

(1) Pecuniary benefit resulting from criminal offences is established by the court by means of a verdict. The pronouncement of the ruling in the part related to the establishment and confiscation of pecuniary benefit resulting from criminal offences shall be explained.

(2) The plaintiff and the counterparty shall have the right to appeal the ruling from paragraph 1 of this Article. A court of higher instance shall rule on the appeal.

Article 5

(1) In addition to contents prescribed by law, in the ruling by means of which the defendant is proclaimed guilty of a criminal offence, the court:

a) shall establish which property or rights represents pecuniary benefit resulting from criminal offences and their monetary equivalent,

b) shall establish that the property or rights have passed into the ownership or have become property of the Republic of Croatia,

c) shall order the counterparty to submit specific property or transfer specific rights to the Republic of Croatia, unless they have already been transferred to the Republic of Croatia based on the provision from point b) of this Article, or to pay their monetary equivalent within 15 days from the date the verdict entered into force.

d) shall determine that rights in favour of the Republic of Croatia are entered in the public registers managed by courts and other bodies.

(2) Unless otherwise prescribed by law, in the verdict by means of which the defendant is acquitted from the charges for criminal offences, or the charges have been dropped except in the case from Article 6 of this Act, the proposal for the confiscation of pecuniary benefit resulting from criminal offences shall be rejected. The court shall also proceed in the above described manner if the defendant has not been acquitted from criminal charges, but the pecuniary benefit is completely covered by the awarded property claim.

(3) The court conducting criminal proceedings has exclusively territorial jurisdiction for reaching the verdict from paragraph 1 of this Article.

Article 6

(1) After the entry into force of the ruling from Article 2, paragraph 3 of this Act, by means of which it decided to conduct the proceedings, the court shall hold a hearing at which the counterparty shall be questioned and other evidence presented. Should it establish that the defendant has perpetrated a criminal offence and acquired pecuniary benefit, the court shall reach the verdict by means of which:

a) it establishes that the defendant has committed a criminal offence,

b) it establishes that by the criminal offence from item a) pecuniary benefit has been acquired as described in Article 3, paragraph 1, point 1 of this Act, and which property or rights represent pecuniary benefit resulting from this offence and its monetary equivalent,

c) it establishes that the property or rights have passed into the ownership, or have become the property of the Republic of Croatia,

d) it orders the counterparty to submit specific property or transfer specific rights to the Republic of Croatia, unless they have already been transferred to the Republic of Croatia based on the provision from item c) of this Article, or to pay their monetary equivalent within 15 days from the date the verdict entered into force.

e) it determines that the rights in favour of the Republic of Croatia are entered in the public registers managed by courts and other bodies.

(2) The proposal from Article 2 paragraph 2 of this Act may be filed until the expiry of the statute of limitation for initiating criminal proceedings as prescribed by the Criminal Code, for an offence from paragraph 1 point a) of this Article. The statute of limitation for filing proposals and conducting criminal proceedings in accordance with this Act may not take effect before the expiry of the period of five years, calculated from the date the criminal offence was committed.

(3) By filing the proposal from Article 2 paragraph 2 of this Act, the course of the statute of limitation is interrupted.

(4) Should the court not establish that the defendant has committed a criminal offence and acquired pecuniary benefit, or the pecuniary benefit is completely covered by the awarded property claim, the court shall proceed in accordance with the provision from Article 5 paragraph 2 of this Act.

(5) If the court has established that objects have been acquired by a criminal offence, which are to be confiscated pursuant to the Act, it shall pass a ruling on the confiscation of the respective objects. Unless otherwise prescribed by law, the ruling shall be passed by the court at which proceedings were conducted when proceedings were concluded or terminated. An appeal may be filed against this ruling. A panel of judges from a court of higher instance shall decide on the appeal.

(6) Proceedings in accordance with paragraph 1 of this Article are conducted in accordance with criminal proceedings rules. A single judge from the court which would be competent for conducting criminal proceedings shall be exclusively competent for reaching the verdict and ruling from paragraphs 1 and 5 of this Article.

Article 7

If criminal proceedings have been terminated before the indictment has been confirmed or during criminal proceedings, and there is probability that pecuniary benefit has been acquired through criminal offences, criminal proceedings pursuant to this Act shall be continued upon proposal by the plaintiff.

Article 8

(1) If legal consequences of initiating bankruptcy proceedings have taken effect, this shall in no way influence provisions of this Act with respect to jurisdiction.

(2) The Republic of Croatia is:

a) a differential creditor related to the enforcement of monetary claims from decisions reached in accordance with provisions of this Act, which have been insured in accordance with Articles 11 to 16 of this Act, unless the respective insurance has been established on property or rights entered into a public register,

b) semifinal lender regarding objects which are its property, based on provisions of Article 5, paragraph 1 and Article 6, paragraph 1 of this Act.

Article 9

(1) Unless otherwise prescribed by law, government bodies, banks and other legal and physical entities shall, upon order of the court, deliver the information related to the establishment of facts necessary for reaching the decisions stipulated by this Act.

(2) When necessary, the court shall order the government bodies and entities from paragraph 1 of this Article to file reports related to the establishment of facts necessary for reaching decisions as described by this Act.

(3) In the order described in paragraphs 1 and 2 of this Article, the court shall define a deadline for delivering the information or filing reports.

(4) For failure to follow the order within the specified period or incomplete execution of the order, the court may, by means of a ruling, sentence a legal entity to a fine in the amount of up to HRK 500,000.00, and a physical entity or a responsible person within a legal entity or government body to a fine in the amount of up to HRK 50,000.00, and if they do not act in accordance with the order even after the described event, they may be sentenced to prison until the fulfilment of the order, for a maximum term of one month.

(5) An appeal against the ruling as described in paragraph 4 of this Article shall not affect its enforcement.

(6) The defendant and their related party can not be punished for failure to fulfil the order from paragraph 1 of this Article.

Article 10

The funds invested into the preparation, perpetration, participation in or covering up of a criminal offence may not be calculated as expenses of the pecuniary benefit resulting from criminal offences.

IV INSURANCE OF THE PECUNIARY BENEFIT CONFISCATION

Article 11

(1) For the purpose of insuring the confiscation of pecuniary benefit resulting from criminal offences, the proponent to insure is authorised to propose insurance by means of any temporary measure for

achieving this purpose before and after initiating criminal proceedings or proceedings from Article 6 of this Act, in particular:

a) by means of prohibiting the confiscation and taxing of real estate or real rights entered on the real estate, with the annotation of the ban entered in the land register, by confiscation of the real estate and entrusting the Office with its keeping and management,

b) by prohibiting the opposing party to confiscate or tax movables, by confiscating this property and entrusting the Office with its keeping,

c) by confiscating and depositing cash and securities and handing them over to the Office,

d) by prohibiting the debtor of the opposing party to voluntarily fulfil their obligation towards the opposing party and by prohibiting the opposing party to receive the fulfilment of the respective obligation, i.e. to access their claims,

e) by order to the bank to withhold the payment of the monetary amount from the account for which a temporary measure has been imposed, to the opposing party or a third party, based on an order by the opposing party,

f) by prohibiting the confiscation and taxing of shares, stakes or business interests, with annotation of the prohibition in the book of shares, stakes or business interests, and upon necessity, also in the public register, by prohibiting the exercise of or access to rights based on such shares, stakes or business interests, by entrusting the Office with the management of stakes, shares or business interests, by appointment of a temporary management for the company,

g) by prohibiting the debtor of the opposing party to submit property, transfer a right or perform another non-monetary action towards the opposing party.

(2) The court from Article 5 paragraph 3, and Article 6 paragraph 6 of this Act shall decide on the proposal for insurance from paragraph 1 of this Article. The ruling needs to contain the term for which the temporary measure has been imposed.

(3) Until charges are brought, the investigating judge shall decide on the proposal from paragraph 1 of this Article, the indictment council shall decide on the proposal after the charges have been brought until their confirmation, and following the confirmation of charges or establishment of the hearing based on a private suit, the court at which the hearing is to be held shall decide on the proposal.

(4) Until proceedings described in Article 6 of this Act have been initiated, the investigating judge shall decide on the proposal from paragraph 1 of this Article, and after they have been initiated, the court at which the hearing is to be held shall decide on the proposal.

(5) An appeal shall be allowed against the ruling from paragraph 2 of this Article within 3 days from its date of delivery. The appeal shall not affect the ruling enforcement. A single judge from a court of the higher instance shall decide on the appeal.

(6) A court or another body appointed by a special law shall be competent for the ruling enforcement.

(7) The ruling from paragraph 2 of this Article shall be immediately delivered to the court or another body competent for its enforcement, at the latest on the next working day following the day on which the ruling has been passed.

(8) The enforcement procedure of the ruling from paragraph 2 of this Article shall be urgent.

Article 12

(1) In the procedure of insurance by means of a temporary measure pursuant to this Act, it shall be presumed that risk exists that the claim of the Republic of Croatia related to the confiscation of pecuniary benefit resulting from criminal offences will not be enforceable, or that the enforcement will be made more difficult if the temporary measure is not imposed.

(2) The insurance can also be established before the opposing party obtained the opportunity to respond to the proponent's proposal to ensure.

Article 13

(1) If it is necessary to enter the temporary measure into a public register (land register, ship register, aircraft register, register of court and notary insurance etc.), the court decision shall also contain the order for entering the temporary measure into a public register.

(2) The proponent to insure is a party to the procedure of entry of the temporary measure into a public register from paragraph 1 of this Article.

(3) No fees shall be paid in the procedure from paragraph 1 of this Article.

Article 14

The legal transaction, by means of which the opposing party disposes of the property or right which is the object of insurance, shall have no legal effect once the temporary measure has been imposed.

Article 15

(1) If the proposal from Article 11, paragraph 1 of this Act has been filed before proceedings have been initiated, the insurance by means of a temporary measure shall be abolished unless charges have been confirmed, the hearing appointed based on a private suit or the proposal from Article 2, paragraph 2 of this Act has been filed, within the period of two years from the date on which the measure has been imposed.

(2) The temporary measure can be abolished or replaced by another measure before expiry of the period for which it has been imposed or before expiry of the term from paragraph 1 of this Article, if the court, upon proposal of the opposing party, establishes that it is unnecessary or that the insurance can be achieved by means of another temporary measure, or if the opposing or third party deposits bail. The bail is always deposited in cash, and exceptionally in property or rights which, according to evaluation by the court, can be monetized within a short period.

(3) If the temporary measure is imposed for a period shorter than the term from paragraph 1 of this Article or the term from Article 16 paragraph 1 of this Act, the opposing party may propose an extension of the temporary measure term.

(4) Provisions of Article 11, paragraphs 2 to 8 of this Act shall apply to the procedure of abolition, extension, replacement or imposition of an additional temporary measure.

Article 16

(1) Insurance by means of a temporary measure may be valid for a maximum of 60 days after the court has delivered information to the proponent to ensure that the verdict from Article 5, paragraph 1 and Article 6, paragraph 1 of this Act has entered into force.

(2) If the verdict from Article 5, paragraph 3 and Article 6, paragraph 1 of this Act was contested by an appeal, the term from paragraph 1 of this Article shall be calculated from the day when the proponent to ensure has received a decision by the court of second instance, by means of which it has been confirmed.

Article 17

(1) The Republic of Croatia is liable for damages arising from the temporary measure imposed for the purpose of confiscating pecuniary benefit resulting from criminal offences.

(2) By way of derogation from paragraph 1 of this Article, if the proposal for the imposition of a temporary measure has been filed by the injured person as plaintiff or a private plaintiff, the injured person or private plaintiff is liable for the damages arising from the temporary measure.

(3) The opposing party may file a lawsuit for the compensation of damages at the competent court, within one year starting from the entry into force of the verdict by means of which the defendant has been acquitted or charges have been dropped, or by means of which the proposal for passing the verdict from Article 6 of this Act has been rejected. In the case from paragraph 1 of this Article, the opposing party may file a lawsuit within 30 days from the day they have been informed that the state attorney had refused their request for a peaceful settlement of the dispute, or from the day when the term in which the state attorney was to reach a decision on the respective request has expired.

V PROTECTION OF THE RIGHTS OF THIRD PARTIES

Article 18

(1) The party from Article 3, paragraph 1, item 11 of this Act has the right to file a complaint until the ruling on the enforcement has been passed, and to demand withdrawal of the temporary measure.

(2) The court which has passed the ruling on the insurance by means of a temporary measure shall decide on the complaint from paragraph 1 of this Article. An appeal may be filed against this ruling within three days from the date of its delivery. An appeal shall not prevent the enforcement of the insurance, as specified by this Act. A single judge from a court of the higher instance shall decide on the appeal.

(3) If a third party proves their right by means of a public document or if the existence of such a right can be established based on the rules on legal presumptions, the appeal shall detain the enforcement of the ruling on insurance by means of a temporary measure.

VI ENFORCEMENT

Article 19

(1) Unless otherwise prescribed by this Act, enforcement for the purpose of confiscating pecuniary benefit resulting from criminal offences shall be established and carried out based on a special law.

(2) The municipal court with territorial jurisdiction which passed the verdict from Article 5, paragraph 1 and Article 6, paragraph 1 of this Act shall be exclusively competent for passing the ruling on establishing enforcement based on the verdict, by means of which pecuniary benefit resulting from criminal offences and misdemeanours is confiscated, and passing other rulings in the course of these criminal proceedings.

(3) The court or body determined by a special law shall be competent for carrying out enforcement based on the ruling from paragraph 2.

(4) If the court from paragraph 2 of this Article is not competent for carrying out enforcement, the rulings from paragraph 2 of this Article shall be delivered to the court or the body competent for carrying out enforcement immediately, and by the latest on the first working day after they have been passed.

VII PROCEDURE WITH TEMPORARILY CONFISCATED PROPERTY AND CONFISCATED PROPERTY

Article 20

(1) Temporarily confiscated monetary funds, submitted property and transferred rights shall be managed by the Office.

(2) The Office shall keep records on temporarily confiscated monetary funds, submitted property and transferred rights.

(3) The minister competent for justice, upon consent of the minister competent for finance, shall adopt the ordinance on keeping the records from paragraph 2 of this Article.

Article 21

(1) The Office may reach the decision on the sale of temporarily confiscated movables without previously issuing a public tender:

a) if their keeping is dangerous, or

b) if there is immediate danger from their deterioration or significant loss of value.

(2) The Office may reach the decision to rent or lease temporarily confiscated objects in accordance with their purpose.

(3) The Republic of Croatia is liable for damages on property from paragraph 2 of this Article caused by rent or lease, in accordance with the general rules on liability for damages.

(4) The Office shall submit the funds obtained through the sale, rent or lease from paragraphs 1 and 2 of this Article to the opposing party within 15 days from the entry into force of the verdict from Articles 5 and 6 of this Act, by means of which the request by the plaintiff was rejected.

(5) The counterparty may file a complaint against the decision of the Office from paragraphs 1 and 2 of this Article within 48 days from its delivery. The court from Article 5, paragraph 3 and Article 6, paragraph 6 of this Act shall decide on the complaint. No appeal against the decision by the court shall be permitted.

Article 22

(1) The Office shall manage and dispose of the property confiscated pursuant to this Act, and in accordance with a special regulation.

(2) Money confiscated in accordance with provisions of this Act and funds obtained through the sale of the property confiscated, in accordance with this Act shall be paid to the state budget.

VIII RIGHTS OF INJURED PERSONS

Article 23

(1) If a property claim has been filed during criminal proceedings, completely or partly adjudicated by the court, or if their is an enforcement decision by the court in a lawsuit, by means of which the request by the injured person related to the criminal offence has been completely or partly accepted, enforcement according to this Act may be established only to the extent to which it will not make the complete settlement of injured persons impossible.

(2) If enforcement has been established contrary to the provision of paragraph 1 of this Article, the injured person in the enforcement procedure for the settlement of claims by the Republic of Croatia, in accordance with provisions of this Act, shall have the status of a third party, demanding that the enforcement be pronounced completely or partially illicit.

Article 24

(1) The Republic of Croatia shall settle the claims of the injured person based on the property claim, only to the amount of the material benefit confiscated in criminal proceedings, pursuant to this Act.

(2) If the injured person has been directed to file a lawsuit or if a lawsuit filed by the injured person who has not filed a property claim is in progress, they shall be authorised to propose a temporary measure within three months from the day they have been informed that the enforcement has been carried out, for the purpose of insuring their claim, with the Republic of Croatia as the opposing party.

(3) The court from Article 19, paragraph 2 of this Act with territorial jurisdiction shall be exclusively competent for passing the ruling on the proposal of the injured person from paragraph 2 of this Article, in criminal proceedings in which provisions of Articles 11 to 17 of this Act shall apply accordingly.

(4) The ruling from paragraph 3 of this Article shall be delivered to the Office, and to parties who have the right to appeal, in accordance with Article 11, paragraph 5 of this Act.

Article 25

Upon proposal of the injured person, the court shall alter or withdraw a temporary measure imposed for the purpose of insuring the confiscation of pecuniary benefit resulting from criminal offences, should this be necessary for insuring the property claim.

IX RECOGNITION AND ENFORCEMENT OF FOREIGN DECISIONS

Article 26

(1) Decisions by foreign bodies, by means of which temporary or similar measures have been imposed regardless of their name, related to the insurance of the confiscation of pecuniary benefit resulting from criminal offences, shall be recognised and enforced on the territory of the Republic of Croatia, in accordance with the international contract.

(2) If no international contract has been concluded with the respective country, the decision by a foreign body shall be recognised:

- if it is not contradictory to the public order of the Republic of Croatia,

- if it has not been made impossible for the opposing party, especially by failure of delivery, to participate in proceedings from which such a decision has arisen,

- if reciprocity exists.

Article 27

(1) Decisions by foreign bodies, by means of which pecuniary benefit resulting from criminal offences was confiscated from the defendant or related parties, shall be recognised and enforced in the territory of the Republic of Croatia, in accordance with the international contract.

(2) If no international contract has been concluded with the respective country, the decision by a foreign body shall be recognised:

- if it is not contradictory to the public order of the Republic of Croatia,

- if it has not been made impossible for the party which the confiscation refers to, especially by failure of delivery, to participate in proceedings from which such a decision has arisen,

- if reciprocity exists.

X SPECIAL CASES OF CONFISCATION

Article 28

(1) Unless otherwise prescribed by law or ordered by the state attorney, objects which were intended or used for the perpetration of a criminal offence or have been created by its perpetration, shall be temporarily confiscated by the police and submitted to the Office. The state attorney shall immediately be informed about this matter, unless the actions are being conducted based on his/her order.

(2) If temporary confiscation has been performed based on the provision of paragraph 1 of this Article, the court which would be competent for passing the ruling on a temporary insurance measure, in accordance with the provision of Article 11, paragraph 4 of this Act, shall rule on the complaint of a third party.

(3) In cases from paragraphs 1 and 2 of this Article, the provisions of Article 18 of this Act shall apply to third parties.

XI AUTHORITY

Article 29

(1) The authority exercised by the state attorney, in accordance with this Act, shall also be exercised by the injured person as plaintiff and a private plaintiff, with the exception of rights and duties exercised by the state attorney as a judicial body.

(2) The authority exercised by the state attorney, in accordance with this Act, shall also be exercised by authorised plaintiffs in accordance with the Misdemeanour Act, with the exception of rights and duties exercised by the state attorney as a judicial body.

(3) In misdemeanour proceedings, decisions shall be reached by the body conducting the misdemeanour proceedings.

(4) The High Misdemeanour Court of the Republic of Croatia shall decide on an appeal against the decision by the body conducting misdemeanour proceedings, reached in accordance with this Act.

XII TRANSITIONAL AND FINAL PROVISIONS

Article 30

From the date the Republic of Croatia has become a full member of the European Union, provisions of Articles 26 and 27 of this Act shall not apply to European Union Member States.

Article 31

(1) Proceedings in cases of ensuring confiscation and reaching decisions on the confiscation of pecuniary benefit resulting from criminal offences, in which a first-instance ruling has been reached before the entry into force of this Act, shall continue based on provisions of the regulations which had been in force at the time when the respective criminal proceedings were initiated.

(2) Provisions of this Act shall apply, if on the day of the entry into force of this Act no decision on ensuring the confiscation or on confiscation of pecuniary benefit resulting from criminal offences, has been reached, or if the first-instance ruling from paragraph 1 of this Article has been annulled and the case returned to the court of first instance for a retrial.

Article 32

The enforcement of valid decisions on the confiscation of pecuniary benefit resulting from criminal offences, reached according to regulations which had been in force before this Act entered into force, shall be carried out in accordance with the regulations which had been valid before its entry into force.

Article 33

The competent minister shall pass the regulation from Article 20, paragraph 3 of this Act within three months from the entry into force of this Act.

Article 34

(1) This Act shall apply to criminal proceedings for criminal offences from Article 21 of the Act on the Office for Combating Corruption and Organised Crime (Official Gazette 76/09 and 116/10), unless otherwise prescribed by the respective Act.

(2) On the day of entry into force of this Act, in the Act on the Office for Combating Corruption and Organised Crime (Official Gazette 76/09 and 116/10), provisions of Article 50, paragraph 3; Article 51, items 3 and 5 – 7; Article 52, paragraph 1, paragraph 3 - second sentence, and paragraph 4; Article 53, paragraphs 3 and 4; Article 54, paragraph 2; Article 55, paragraph 1, item 4, and paragraphs 2 – 5; Article 56, paragraph 1, item 5 and paragraph 5; Article 57, paragraphs 6 and 7; Article 58 and Article 60, paragraph 1 shall become invalid.

Article 35

This Act shall enter into force on the eighth day from the date of its publishing in the Official Gazette.

ANNEX VII Act on the Responsibility of Legal Person for the Criminal Offences

Application of criminal legislation
Article 2

Unless otherwise prescribed by this Act, the provisions of the Criminal Code, the Criminal Procedure Act and the Law on the Office for the Prevention of Corruption and Organized Crime shall apply to legal persons.

Foundation of responsibility of legal persons
Article 3

(1) The legal person shall be punished for a criminal offence of a responsible person if such offence violates any of the duties of the legal person or if the legal person has derived or should have derived illegal gain for itself or third person.

(2) Under the conditions referred to in paragraph 1 of this Article the legal person shall be punished for the criminal offences prescribed by the Criminal Code and other laws prescribing the criminal offences.

Amount of a fine
Article 10

(1) If the criminal offence is punishable by imprisonment for a term of up to one year, the legal person may be punished by a fine of 5.000,00 to 5.000.000,00 kuna.

(2) If the criminal offence is punishable by imprisonment for a term of up to 5 years, legal person may be punished by a fine of 10.000,00 to 6.000.000,00 kuna.

(3) If the criminal offence is punishable by imprisonment for term of up to 10 years, legal person may be punished by a fine of 15.000,00 to 7.000.000,00 kuna.

(4) If the criminal offence is punishable by imprisonment for a term of up to 15 years or by long-term imprisonment, the legal person may be punished by a fine of 20.000,00 to 8.000.000,00 kuna.

Termination of legal person
Article 12

(1) The penalty of termination of the legal person may be pronounced if the legal person has been established for the purpose of committing criminal offences or if the same has used its activities primarily to commit criminal offences.

(2) The penalty of termination of the legal person may not be pronounced on units of local and regional self-government, political parties and trade unions.

(3) Apart from the penalty of termination of the legal person the court may also impose a fine upon the legal person.

(4) After the judgement on termination of the legal person becomes final, liquidation shall be carried out.

Types of security measures
Article 15

Apart from other penalties the court may impose one or more of the following security measures on the legal person: ban on performance of certain activities or transactions, ban on obtaining of licenses, authorizations, concessions or subventions, ban on transaction with beneficiaries of the national or local budgets, and confiscation.

Confiscation
Article 19

The security measure of confiscation is imposed under the conditions referred to in Article 80 of the Criminal Code.

Confiscation of illegally gained benefit
Article 20

(1) The court shall confiscate from the legal person the illegally gained benefit as a proceeds of the criminal offence.

(2) The illegally gained benefit referred to in paragraph 1 of this Article means any increase or prevention of a decrease of the legal person's property in consequence of the commission of a criminal offence.

(3) The illegally gained benefit obtained in consequence of the commission of a criminal offence shall be confiscated on the basis of the judgement which establishes the commission of the criminal offence. The amount of the illegally gained benefit shall be determined by the court after studying the entire property of the legal person and relation of the same to the offence committed..

(4) Should it be established that it is impossible to confiscate the illegally gained benefit consisting in money, rights or objects, the court shall oblige the legal person to pay the full replacement value in money. In determination of such value in money the court shall take into consideration the market value of material assets or rights at the moment of judgement.

(5) The illegally gained benefit shall be confiscated also in cases when it is kept by third persons on the basis of any right whatsoever, if under the circumstances of such gain the same knew or could know and was/were supposed to know that the value was gained in consequence of the commission of a criminal offence.

ANNEX VIII Act on International Restrictive Measures

THE CROATIAN PARLIAMENT

3885

Pursuant to Article 88 of the Constitution of the Republic of Croatia, I hereby issue the

DECISION
PROMULGATING THE ACT
ON INTERNATIONAL RESTRICTIVE MEASURES

I hereby promulgate the Act on International Restrictive Measures, passed by the Croatian Parliament at its session on 21 November 2008.
Class: 011-01/08-01/149
Reg. No: 71-05-03/1-08-2
Zagreb, 27 November 2008

The President of the Republic of Croatia
Stjepan Mesić, m.p.

ACT
ON INTERNATIONAL RESTRICTIVE MEASURES

Article 1

This Act regulates the procedure of introduction, application and abolition of international restrictive measures that the Republic of Croatia introduces, applies and abolishes in line with international acts and decisions accepted within the framework of international organisations, with the objective of establishing and/or maintaining international peace and security, respecting human rights and fundamental freedoms, developing and strengthening democracy and state of law, and other objectives harmonised with international law.

Article 2

(1) Restrictive measures are:

a) restrictions or obligations towards states, international organisations, natural and legal persons and other entities that may be comprised by international restrictive measures laid down in legal acts of the United Nations, the European Union or the European Community and other international organisations which are binding for the Republic of Croatia, and
b) restrictions or obligations introduced by the Republic of Croatia in another manner, in line with international law or the law of the European Union.

(2) Restrictive measures may be as follows:

a) severance of diplomatic relations,
b) total or partial termination of economic relations,
c) total or partial restriction of import, export, transit, provision of services, and of transport, mail and other communications,
d) arms embargo,
e) restriction upon entry into the country,
f) restricted disposal of assets, and
g) other measures in line with international law.

Article 3

(1) Assets, for the purposes of this Act, are all means, tangible or intangible, movable or immovable, as well as documents or instruments in any form, including the electronic and digital form, which prove the ownership or right to ownership of assets.

(2) Funds, for the purposes of this Act, are financial means and benefits of any kind, including the following:

a) cash, cheques, financial claims, bills of exchange, remittances and other methods of payment,

b) funds invested with liable persons referred to in Article 10 paragraph 1 of this Act,
c) financial instruments determined by the law regulating the capital market, used for trading in public or private offerings, including shares, certificates, debt instruments, bonds, guarantees and derived financial instruments,
d) other documents proving the right to financial means or other financial resources,
e) interest rates, dividends and other funds-related income,
f) claims, loans and letters of credit.

Article 4

(1) The Government of the Republic of Croatia (hereinafter: the Government) shall issue a decision on the introduction of restrictive measures, prescribing the application of the restrictive measures on a case-by-case basis and determining the type of the restrictive measure, the manner of its application, the duration period and supervision of its application.

(2) Restrictive measures shall be abolished by the Government's decision.

(3) The decisions referred to in paragraphs 1 and 2 of this Article shall be published in the Official Gazette.

Article 5

(1) The Government shall establish the Standing Coordination Group for Monitoring the Implementation of International Restrictive Measures to monitor and coordinate application of the restrictive measures referred to in this Act (hereinafter: Group). In the decision on establishing the Group, the Government shall regulate in detail the organisation, authorisations, methods and rules of procedure of the Group, which will be headed by a representative of the ministry in charge of foreign affairs (hereinafter: Ministry).

(2) In order to be able to efficiently propose the monitoring and coordination of application of the restrictive measures under this Act, the Group may process data from the Database.

Article 6

(1) With the aim of efficient application of restrictive measures and international data exchange, the Government shall pass a decision on establishing the Database on restrictive measures, natural and legal persons and other entities to whom the restrictive measures apply (hereinafter: Database), prescribing the method of keeping and maintaining the Database and processing the data.

(2) The Database shall be established, kept and maintained by the Ministry.

(3) The Database of natural persons shall contain the following information: person's name and surname, date and place of birth, place of permanent residence or temporary residence, nationality, type and number of identity papers, registration number or personal identification number (after its determination and assignment), data on the assets, proprietary rights and obligations of the person in the territory of the Republic of Croatia, date of commencement and date of termination of a specific restrictive measure, restrictive measures which have been taken, and data on reasonable suspicion regarding violation or attempted violation of a restrictive measure.

(4) The Database of legal persons and other entities shall contain the following information: legal person's name and head office, name and surname of its authorised representative, registration number (MBS), tax number (MB) or personal identification number (after its determination and assignment), data on the assets, proprietary rights and obligations of the person in the territory of the Republic of Croatia, date of commencement and of termination of a specific restrictive measure, restrictive measures which have been taken, and data on reasonable suspicion regarding violation or attempted violation of a restrictive measure.

(5) The data referred to in paragraphs 3 and 4 of this Article shall be kept for five years after the abolishment of a restrictive measure. Upon the expiry of this deadline, the data shall be erased or destroyed in line with regulations regulating personal data protection and regulations regulating data secrecy, or they shall be filed pursuant to regulations regulating safety of filed documents.

(6) The Ministry may deliver the data from the Database to the international organisations referred to in Article 2 paragraph 1 of this Act, at their request.

Article 7

(1) Natural and legal persons and other entities shall be entitled to insight into the data from the Database referring to them, in line with regulations regulating data secrecy protection and personal data protection.

(2) Within three months from the day of publication of the notification on abolishment of restrictive measures in the Official Gazette, natural persons shall be informed about their right to insight into the data which were collected unbeknownst to them and which have not been erased from the Database.

Article 8

(1) In the procedure of deciding upon petitions submitted by persons pursuant to regulations passed on the basis of this Act, provisions of the Act on General Administrative Proceedings shall apply.

(2) The petitions referred to in paragraph 1 of this Article shall be decided upon by the ministry competent for the area to which the petitions refer.

(3) The Ministry deciding on the petitions referred to in paragraph 1 of this Article may, prior to making the decision, request the Group's opinion regarding the petition.

Article 9

(1) For damage caused as the result of application of this Act, it shall not be possible to claim compensation from the Republic of Croatia or the persons applying restrictive measures.

(2) As an exception, the provision of paragraph 1 of this Article shall not apply if the damage was caused on purpose or by gross negligence.

Article 10

(1) Natural and legal persons and other entities shall be obliged to act in line with this Act, to ensure direct application of restrictive measures within their scope of activities, and to notify the Ministry thereof.

(2) The natural and legal persons and other entities referred to in paragraph 1 of this Act, as well as state administration bodies, shall submit to the Ministry, at its request, the data referred to in Article 6 paragraphs 3 and 4 of this Act, which are at their disposal.

Article 11

(1) Restricted disposal of assets shall be implemented by applying the following measures for freezing the assets:

a) freezing of all the assets owned, held or belonging in any other way to the entity to whom the measures are applied, or controlled or supervised by that entity,
b) making the assets unavailable, directly or indirectly, to the entity to whom the measures are applied,
c) prohibition of all actions whose direct or indirect aim is to consciously avoid the measures referred to in items a) and b) of this paragraph.

(2) The provision of paragraph 1 item b) of this Article shall not refer to inflow to frozen accounts based on interest rates or other income of those accounts, provided that the provision of paragraph 1 item a) of this Article still applies to all such interest rates or income.

(3) The provision of paragraph 1 item b) of this Article shall not prevent inflow of funds transferred by third persons to the frozen account of the entity to which restrictive measures apply, provided that all such inflows to the account are also frozen.

Article 12

(1) By way of derogation from the provisions of Article 11 paragraph 1 of this Act, the court may allow the frozen assets to be released or the funds in question made available if it has been established

that they are necessary for covering the basic costs of living, rent, lease or mortgage on a house of flat, medicines and treatment, taxes and insurance, or costs of public utility services.

(2) By way of derogation from the provisions of Article 11 paragraph 1 of this Act, the court may allow the frozen assets to be released or made available if it has been established that the assets are:

a) intended exclusively for payment of fees for regular maintenance of the frozen assets,
b) necessary due to extraordinary expenses, such as expenses related to childbirth, death in the family or a similar event.

(3) When deciding pursuant to paragraphs 1 and 2 of this Article, the court may determine conditions under which the release or the making available of assets will be approved.

(4) The competent court shall inform the Ministry about the approval referred to in this Article eight days after the issuance of the approval at the latest.

(5) The Ministry shall inform competent bodies of international organisations which apply the same restrictive measures towards the same entities about each approval decided upon pursuant to this Article.

Article 13

Supervision of implementation of this Act and regulations passed on the basis thereof shall be carried out by competent state administration bodies and holders of public authorities competent for the area to which the restrictive measures refer.

Article 14

In case of suspicion that violation or attempted violation of restrictive measures contains elements of a criminal act or any other punishable act, data kept in the Database referred to in Article 6 paragraph 2 of this Act shall be delivered to state bodies competent for detection of misdemeanours or crimes and for initiating proceedings.

Article 15

(1) Any person not acting in accordance with the Government's decision determining the restrictive measures referred to in Article 2 paragraph 2 items c) and d) of this Act shall be punished by a fine or prison sentence lasting from six months to five years.

(2) Any person not acting in accordance with the Government’s decision determining the restrictive measures referred to in Article 2 paragraph 2 items a), b), e) and f) of this Act shall be punished by a fine or prison sentence lasting up to three years.

(3) Any person committing the criminal act referred to in paragraphs 1 and 2 of this Article by negligence shall be punished by a fine or prison sentence lasting up to six months.

(4) For the attempted crime referred to in paragraph 2 of this Article, the perpetrator shall be punished.

Article 16

(1) Legal persons that do not notify the Ministry in line with the provision of Article 10 paragraph 1 of this Act or that do not submit data to the Ministry in line with the provision of Article 10 paragraph 2 of this Article shall be fined for a misdemeanour in the amount from HRK 150,000 to 1,000,000.

(2) A member of the management board or another responsible person in the legal person shall be fined for the misdemeanour referred to in paragraph 1 of this Article in the amount from HRK 15,000 to 50,000.

(3) Natural persons shall be fined for the misdemeanour referred to in paragraph 1 of this Article in the amount from HRK 15,000 to 50,000.

(4) Self-employed natural persons who have committed the misdemeanour referred to in paragraph 1 of this Article while performing his/her activities shall be fined in the amount from HRK 50,000 to 500,000.

Article 17

(1) The Government shall issue a decision on establishing the Group referred to in Article 5 paragraph 1 of this Act within six months from the entry into force thereof.

(2) The Inter-Ministerial Group for Monitoring the Implementation of International Restrictive Measures, established by the Decision of the Government of the Republic of Croatia of 24 February 2005 (Class: 022- 03/05-02/12, Reg. No: 5030102-05-1), amended by the Government's Decision of 14 September 2006 (Class: 022-03/06-02/32, Reg. No: 5030106-06-1) shall, upon the entry into force of this Act, continue working until the decision referred to in paragraph 1 of this Article has been issued.

Article 18

Restrictive measures adopted on the basis of the Act on International Restrictive Measures (Official Gazette 178/04) shall remain in force until the passing of a decision on their abolishment in line with the provisions of Article 4 paragraph 2 of this Act.

Article 19

On the date of the entry into force of this Act, the Act on International Restrictive Measures (Official Gazette 178/04) shall cease to have effect.

Article 20

This Act shall enter into force on the eighth day after the day of its publication in the Official Gazette.

Class: 018-02/08-01/02
Zagreb, 21 November 2008

THE CROATIAN PARLIAMENT
The President of the Croatian Parliament
Luka Bebić, m.p.

ANNEX IX Confiscation of Pecuniary Gain Acquired by a Criminal Offence in 2011

Confiscations recorded at County and Municipal State Attorneys' Offices in 2011

Criminal Offence	No. of security measures	Amount secured through freezing	No. court rulings	Amounts
Art. 173.st.2 CC			67	1,247,888
Art. 177. CC			1	2,200
Art. 195. CC			26	878,997
Art. 216.1 CC	9	10,237	201	540,223
Art. 217/1 CC	3	40,433	357	2,418,106
Art. 218. CC			62	477,166
Art.219. CC			3	3,536
Art. 220. CC	1	424,163	8	1,483,945
Art. 224. CC	7	5,819,216	103	8,784,169
Art. 224.a CC			10	79,005
Art. 226			2	31,043
Art. 227. CC			2	155,419
Art. 330. CC			1	503
Art. 234. CC			7	163,368
Art. 235. CC			2	3,600
Art. 236. CC			5	5,622
Art. 259. CC			1	421
Art. 261. CC	1	51,915,390		
Art. 274. CC			1	3,000
Art. 282 CC	1	28,484,546		
Art. 286. CC			4	4,571,147
Art. 287. CC			1	30,000
Art. 292. CC	2	52,537,518	25	18,679,547

Art. 293 CC	1	2,000,000	13	3,318,253
Art. 297. CC			1	15,000
Art. 298 CC			5	
Art. 311. CC			2	18,560
Art. 317. CC			1	800
Art. 330. CC			1	503
Art. 337. CC	42	66,964,467	32	16,818,108
Art. 344. CC	1	642,479		
Art. 345. CC			19	1,039,890
Art. 33 Law on Energy			2	15,222
Total	68	208,838,452	965	60,785,249

USKOK

Criminal Offence	No. of security measures	Amount secured through freezing	No. court rulings	Amounts
Art. 294.a CC	1	5,625,212		
Art. 177/3 CC			7	1,582,229
Art. 173/3 CC	1	940,000	10	11,891,908
Art. 218/2 CC			1	316,119
Art. 298/1 CC			5	771,003
Art. 333/3 i 217/2 CC	1	690,901	3	222,126
Art.337. CC	8	22,478,964	7	307,706
Art. 343/1 CC	1		3	1,196,889
Art. 347. CC	2	17,000,000	14	1,152,699
Art. 348. CC			5	865,789
Total	14	46,735,077	55	18,306,474

Grand total

USKOK and State Attorney's Office	No. of security Measures	Amount secured through freezing	No. court rulings	Amounts
Grand total	82	255,.573,530	1,020	79,091,723

ANNEX X Credit Institutions Act

Credit institution

Article 2

(1) 'Credit institution' means a legal person authorised by the competent authority, whose business is to receive deposits and other repayable funds from the public and to grant credits for its own account.

(2) A credit institution having its registered office in the Republic of Croatia may, under the conditions laid down in this Act, be established as a bank, savings bank or a housing savings bank.

(3) For the purposes of this Act, the term 'credit institution', where not further qualified by the words 'of a Member State' or 'of a third country', means a credit institution which has its registered office in the Republic of Croatia and is authorised by the Croatian National Bank. Exceptionally, for the purposes of this Title, the term 'credit institution' shall be used for all credit institutions regardless of the country where they have their registered office. For the purposes of Title XXIII Supervision on a consolidated basis, the term 'subsidiary credit institution' shall be used for any credit institution having the status of a subsidiary credit institution regardless of the country where it has its registered office.

Initial capital of a credit institution

Article 29

(1) The initial capital of a bank shall not be less than HRK 40 million.

(2) The initial capital of a savings bank shall not be less than HRK 8 million.

(3) The initial capital of a housing savings bank shall not be less than HRK 20 million.

Approval to acquire a qualifying holding

Article 34

(1) A legal or natural person, the group of connected persons referred to in Article 24 of this Act and persons acting in concert pursuant to Article 25 of this Act, shall obtain prior approval from the Croatian National Bank for the acquisition of shares of a credit institution on the basis of which they, individually or jointly, directly or indirectly, acquire a qualifying holding in the credit institution.

(2) Holders of a qualifying holding shall obtain prior approval from the Croatian National Bank for each further direct or indirect acquisition of shares of a credit institution on the basis of which their holding would reach or exceed 20 percent, 30 percent or 50 percent of the capital or of the voting rights of a credit institution.

(3) Persons who obtained the prior approval referred to in paragraphs (1) and (2) of this Article shall, within 12 months of the adoption of the decision on the prior approval, complete the acquisition of a qualifying holding and the holding referred to in paragraph (2) of this Article and notify the Croatian National Bank thereof.

(4) Should persons who obtained the prior approval referred to in paragraphs (1) and (2) of this Article take a decision to sell or otherwise dispose of their shares so as to reduce their holdings below the threshold for which they obtained prior approval, they shall notify the Croatian National Bank in advance.

(5) Persons who have obtained the prior approval referred to in paragraphs (1) and (2) of this Article, and who have thereafter sold or otherwise disposed of their shares and thereby reduced their holdings below the threshold for which they obtained prior approval, shall submit an application to the Croatian National Bank for prior approval to acquire a qualifying holding or the holding referred to in paragraph (2) of this Article if, following the expiry of a period of 12 months of the adoption of the

decision on the prior approval, they again intend to acquire a qualifying holding or the holding referred to in paragraph (2) of this Article in the amount for which they obtained prior approval.

(6) Before adopting a decision whether to grant prior approval to acquire a qualifying holding or the holding referred to in paragraph (2) of this Article, the Croatian National Bank shall consult the competent supervisory authority if the acquirer is one of the following:

1) a credit institution, an insurance or reinsurance undertaking or an asset management company within the meaning of the law governing the operation of investment funds (hereinafter: asset management company), a pension company within the meaning of the law governing the operation of pension funds (hereinafter: pension company), an investment firm authorised in another Member State, or if the acquisition falls within the competence of another supervisory authority;

2) the parent undertaking of a credit institution, an insurance or reinsurance undertaking, an asset management company, a pension company, or an investment firm authorised in another Member State, or if the acquisition falls within the competence of another supervisory authority; or

3) a natural or legal person controlling a credit institution, an insurance or reinsurance undertaking, an asset management company, a pension company or an investment firm authorised in another Member State, or if the acquisition falls within the competence of another supervisory authority.

(7) Legal persons holding qualifying holdings shall notify the Croatian National Bank of any changes in their status, including participation in mergers, acquisitions or divisions, within eight days of effecting such changes.

(8) A financial holding company or mixed-activity financial holding company which, in accordance with the approval to acquire a qualifying holding, has the status of the parent undertaking of a credit institution, shall notify the Croatian National Bank of any change in its management board within eight days of effecting the change.

(9) The provisions on the percentage of voting rights of the law governing the capital market shall be applied mutatis mutandis to determine the percentages referred to in paragraphs (1) and (2) of this Article.

(10) Voting rights or shares which credit institutions may hold as a result of providing the underwriting of financial instruments and/or placing of financial instruments on a firm commitment basis shall not be taken into account when determining the size of a qualifying holding or the holding referred to in paragraph (2) of this Article, provided that those rights are, on the one hand, not used to intervene in the management of the issuer and, on the other, disposed of within one year of acquisition.

(11)5 Shareholders of a credit institution who, after acquiring shares of the credit institution become connected persons pursuant to Article 24 or persons acting in concert pursuant to Article 25 of this Act, owing to which they as a group of connected persons or persons acting in concert jointly hold 10 percent, 20 percent, 30 percent or 50 percent of the capital or of the voting rights of the credit institution, shall submit to the Croatian National Bank an application to acquire a qualifying holding within 30 days of the date when they became connected persons or persons acting in concert. If they fail to do so, the Croatian National Bank shall act in accordance with Article 40, paragraph (2) of this Act.

(12) Should qualifying holdings increase due to the reduction in the initial capital of the credit institution or other similar action by the credit institution so as to exceed 10 percent, 20 percent, 30 percent or 50 percent, holders of qualifying holdings shall submit an application for further acquisition of a holding in the capital or of the voting rights of the credit institution within 30 days of the date when they became aware or should have become aware of the increase in their holdings due to the credit institution's action. If they fail to do so, the Croatian National Bank shall act in accordance with Article 40, paragraph (2) of this Act.

(13) The provisions of this Title shall apply mutatis mutandis to the holders of qualifying holdings referred to in paragraphs (11) and (12) of this Article.

Application to acquire a qualifying holding
Article 35

(1) An application for prior approval to acquire a qualifying holding shall be accompanied by:

1) for an acquirer of a qualifying holding that is a legal person:

a) a certificate from the register of companies or other relevant register, in the form of an original or a certified copy not older than three months;

b) a certificate from the register of shareholders (book of shares) or book of holdings, in the form of an original or a certified copy;

c) a list of natural persons who are the ultimate shareholders of the acquirer or holders of holdings in the acquirer, listing the following data: name, address or domicile, other data for identification, the total nominal value of the shares and percentage of the initial capital of the acquirer, and information referred to in paragraph (1), item (2) under (b) and (c) of this Article;

d) a list of persons connected in the manner referred to in Article 24 of this Act with the acquirer and the manner in which they are connected;

e) audited financial statements of the acquirer for the two preceding years of business;

f) evidence on the availability of funds for the acquisition of a qualifying holding and a description of the method or source of financing;

g) a description of the requested prior approval, including the total nominal value of the shares and percentage of the initial capital of the credit institution in which the qualifying holding is to be acquired, explanation of the objectives to be achieved by the acquisition of the qualifying holding and the strategic direction of the acquirer in relation to holdings in credit and financial institutions;

h) a description of the acquirer's activities in relation to the acquisition preceding the application;

i) proof that the acquirer has not committed a crime;

j) evidence that bankruptcy proceedings have not been initiated or opened against the property of the acquirer;

k) an opinion or approval of the competent authority of a credit institution of a Member State or a third country in relation to the proposed acquisition; and

l) for an acquirer of a qualifying holding that is a financial holding company, evidence that the criteria referred to in Article 45 of this Act have been met;

2) for an acquirer of a qualifying holding who is a natural person:

a) name, address or domicile, and other data for identification;

b) curriculum vitae of the acquirer, listing all companies, and their addresses, with whom he/she is or was employed, of which he/she is or was a member of the management or supervisory board, or in which he/she is or was a holder of a qualifying holding;

c) evidence that the person has not been convicted by a final judgement of a crime against the values protected by international law or of one of the following crimes:

– against the payment system and the security of its operations;

– relating to the authenticity of documents;

– relating to breaches of official duties;

– relating to money laundering; or

– relating to terrorist financing; and

d) documents referred to in item (1) under (d), (f), (g) and (h) of this paragraph.

(2) By way of derogation from paragraph (1), item (1) under (i) and item (2) under (c) of this Article, the Croatian National Bank shall obtain proof from the criminal history records that the domestic natural person has not committed a crime. For a natural person who is not a citizen of the Republic of Croatia, the Croatian National Bank shall obtain proof from the criminal history records that the person has not committed a crime in the Republic of Croatia. The Croatian National Bank must provide a reasoned explanation for each request from the records.

(3) Where the acquisition of a qualifying holding may result in dominant influence over or control of the credit institution's operation, in addition to the documents referred to in paragraph (1), item (1) or (2) of this Article, the acquirer shall enclose the following with the application:

1) a business strategy of the credit institution in which the qualifying holding is acquired;

2) a business plan for the next three years of business, including balance sheets and profit and loss accounts;

3) planned changes in the organisational, management and personnel structure of the credit institution;

4) a plan of activities regarding the creation of new internal bylaws, or amendments to the existing internal bylaws of the credit institution; and

5) a plan of activities regarding the changes to the existing information technology or implementation of new information technology of the credit institution.

(4) In addition to the documents referred to in paragraphs (1) and (3) of this Article, the Croatian National Bank may request additional documentation that it deems necessary to decide whether to grant prior approval, including information prescribed in the law regulating the prevention of money laundering and terrorist financing, which is being collected by the persons subject to that law.

(5) When deciding whether to grant prior approval to acquire a qualifying holding and the holding referred to in Article 34 of this Act, the Croatian National Bank shall examine the suitability of the sources of funds which the acquirer intends to use for the acquisition of a qualifying holding in a credit institution.

(6) The Croatian National Bank may, for the purpose of obtaining information necessary to decide whether to grant prior approval to acquire a qualifying holding, verify the data delivered by the acquirer of a qualifying holding.

Management board
Article 43

(1) The management board of a credit institution shall have at least two members who direct the business of the credit institution and represent it. One of the members of the management board shall be appointed chairperson of the management board.

(2) The management board shall direct the business of a credit institution from the territory of the Republic of Croatia.

(3) Unless provided otherwise in the Articles of Association, members of the management board of a credit institution shall jointly direct the business of the credit institution and jointly represent it.

(4) The management board of a credit institution may authorise one or more procurators to represent the credit institution, conclude contracts and perform legal acts in the name and for the account of the credit institution, which arise from the services for which the credit institution obtained authorisation from the Croatian National Bank, but they may only do so jointly with at least one member of the credit institution's management board.

(5) When entering the name of a procurator in the register of companies, the credit institution's management board shall also enter the limitations on the powers of the procurator.

(6) The conditions that procurators must fulfil, the manner in which procurators are named, the powers of procurators, and any limitations on actions that procurators may take, shall be defined in the Articles of Association of a credit institution.

(7) At least one member of the management board of a credit institution shall have command of the Croatian language sufficient for performing this function.

Eligibility for management board membership
Article 45

(1) Members of the credit institution's management board must meet the following criteria:

1) they possess an undergraduate degree pursuant to regulations governing scientific activity and higher education;

2) they possess professional qualifications, abilities and experience appropriate and adequate to direct the business of a credit institution;

3) they have not held management positions in a credit institution or undertaking against which bankruptcy or compulsory winding-up proceedings have been opened or whose authorisation has been withdrawn;

4) they are not members of the supervisory board of that credit institution or the supervisory board of any other credit institution entered in the register of companies in the Republic of Croatia;

5) they have not had bankruptcy proceedings opened against their personal property;

6) they have a good reputation;

7) they have not been convicted by a final judgement of a crime against the values protected by international law or of one of the following crimes:

– against the payment system and the security of its operations;

– relating to the authenticity of documents;

– relating to breaches of official duties;

– relating to disclosure of a state secret;

– relating to money laundering; or

– relating to terrorist financing;

8) based on their conduct thus far it may be reasonably concluded that they will perform the duties of members of the credit institution's management board diligently and conscientiously,

9) they meet the eligibility criteria for management board members prescribed in Article 239, paragraph (2) of the Companies Act; and

10) they are not members of the management board or procurators of another undertaking.

(2) The experience referred to in paragraph (1), item (2) of this Article shall mean at least three years experience in management positions in a credit institution or five years experience in directing a business comparable to the activities of credit institutions or other comparable activities.

(3) It shall be deemed that a natural person who is not a citizen of the Republic of Croatia meets the criteria referred to in paragraph (1), items (7) and (9) of this Article if the person has not been convicted by a final judgement of a crime which by definition corresponds to these crimes.

(4) By way of derogation from paragraph (1), item (3) of this Article, persons who held management positions in an undertaking or a credit institution against which bankruptcy or compulsory winding-up proceedings have been opened or whose authorisation has been withdrawn may be appointed to the management board of a credit institution if the Croatian National Bank assesses that the actions of such persons did not contribute to the events referred to in paragraph (1), item (3) of this Article.

(5) By way of derogation from paragraph (1), item (4) of this Article, members of the supervisory board of a subsidiary credit institution may be appointed to the management board of the parent credit institution.

(6) The Croatian National Bank shall prescribe in detail the eligibility criteria for management board membership referred to in paragraphs (1) and (2) of this Article, the procedure for issuing prior approvals and the documentation to be enclosed with the application for prior approval for the chairperson or member of the management board.

Banking secrecy

Article 168

(1) 'Banking secrecy' means a credit institution's obligation to protect the confidentiality of all information, facts and circumstances of which it becomes aware in the course of providing services to clients or in the course of business with individual clients. Credit institutions shall be bound by the obligation of banking secrecy.

(2) For the purposes of this Act, a credit institution's clients shall be all persons who requested or received banking and/or financial services from the credit institution.

Obligation of banking secrecy

Article 169

(1) Members of the credit institution's bodies, its shareholders or employees and other persons who, due to the nature of their business with or for the credit institution have access to confidential information, shall be bound by the obligation of banking secrecy. They may not divulge confidential information to third parties, use it against the interests of the credit institution or its clients, or enable third parties to make use of it.

(2) The persons referred to in paragraph (1) of this Article shall be bound by the obligation of banking secrecy even after the termination of their employment with the credit institution or after the termination of their status of shareholders or membership in the credit institution's bodies, as well as after the termination of their contract on the performance of activities for the credit institution.

(3) The credit institution's obligation of banking secrecy shall not include the following cases:

1) where the client explicitly agrees in writing that certain confidential information may be disclosed;

2) where this enables the credit institution to realise its interest when exercising the sale of its receivables;

3) where confidential information is disclosed to the Croatian National Bank, the Financial Inspectorate of the Republic of Croatia or another supervisory authority for the purposes of supervision or oversight within their competence;

4) where confidential information is exchanged within a group of credit institutions for the purpose of risk management;

5) where confidential information is disclosed to a legal person established pursuant to a special law to collect and disseminate information on the creditworthiness of legal and natural persons;

6) where credit and/or financial institutions exchange confidential information on clients who defaulted on their obligations, and where such information is disclosed to a legal person established to collect and disseminate such information;

7) where the disclosure of confidential information is essential for collecting and establishing facts in criminal or preliminary proceedings, when requested or ordered in writing by the competent court;

8) where the disclosure of confidential information is necessary to carry out foreclosure or bankruptcy proceedings over the property of a client, legacy proceedings or other property-rights proceedings, and such disclosure is requested or ordered in writing by the competent court or public notary in the course of performing the functions entrusted to them pursuant to law;

9) where the interests or obligations of a credit institution or its client require the disclosure of confidential information to establish the legal relationship between the credit institution and the client in court proceedings, arbitration proceedings or conciliation proceedings;

10) where confidential information is disclosed to the Office for the Prevention of Money Laundering pursuant to the law governing the prevention of money laundering and terrorist financing;

11) where confidential information is disclosed to the Office for the Prevention of Corruption and Organised Crime pursuant to the law governing the prevention of corruption and organised crime;

12) where confidential information is required by the tax authorities in procedures carried out within the framework of their competence under law, and is disclosed at their written request;

13) where confidential information is disclosed to the institution responsible for deposit insurance pursuant to the law governing deposit insurance;

14) where the account balance reflects inability to effect payments and the certificate is requested to substantiate the existence of grounds for bankruptcy;

15) disclosure of information to insurance undertakings within the procedure of insuring the credit institution's receivables;

16) disclosure of information in the course of concluding legal arrangements which have the effect of insuring the credit institution's receivables, such as derivative credit instruments, bank guarantees and similar arrangements;

17) disclosure of information, subject to written consent of the credit institution's management board, to a holder of a qualifying holding in the credit institution, to a person intending to acquire a qualifying holding in the credit institution, to a person who acquires the credit institution or with whom the credit institution merges, to a legal person intending to take over the credit institution as well as to auditors, legal and other experts authorised by a holder of a qualifying holding or a potential holder;

18) disclosure of information necessary for the exercise of the credit institution's activities which are subject to outsourcing, where information is disclosed to the providers of outsourced activities;

19) where a credit institution which provides services of storing and administering financial instruments for the account of clients, including custody services, discloses information on the holder of securities to a credit institution which is the issuer of these non-material securities at its request;

20) where confidential information is disclosed to social welfare centres at their written request, within the framework of their competence under law and for the purpose of taking measures to protect the rights of children (persons under 18) and persons under guardianship; and

21) where so provided for in other laws.

(4) Disclosure of confidential information shall not be considered to include:

1) disclosure of information in collective form, such that personal or business data on a client cannot be identified; and

2) disclosure of public information from the unified register of accounts.

(5) The credit institution shall ensure that when concluding each individual contract on the provision of banking and/or financial services, the client's explicit agreement in writing referred to in paragraph (3), item (1) of this Article is given in a separate document.

Use and protection of confidential information

Article 170

(1) The Croatian National Bank, courts, other supervisory authorities and other persons referred to in Article 169, paragraph (3) of this Act, shall use the confidential information they have received under the same Article exclusively for the purpose for which it has been given and may not divulge it to third parties or enable third parties to acquire and make use of such information, except in cases prescribed by law.

(2) The provision of paragraph (1) of this Article shall also apply to all natural persons who work or have worked for the Croatian National Bank, the courts, other supervisory authorities or other persons referred to in Article 169, paragraph (3) of this Act in the capacity of employees or other capacities.

Bookkeeping documents

Article 172

(1) A credit institution shall prepare, check and store bookkeeping documents in accordance with applicable regulations and professional standards.

(2) By way of derogation from paragraph (1) of this Article, a credit institution shall store for a period of at least eleven years:

1) documents relating to the opening, closing and recording of changes in payment system and deposit accounts;

2) documents relating to other changes not covered by item (1) of this paragraph on the basis of which data have been entered in the credit institution's business books; and

3) contracts and other documents relating to the establishment of a business relationship.

(3) The time limit referred to in paragraph (2) of this Article shall mean the period following the end of the year in which the business change occurred, i.e. in which bookkeeping documents were prepared. Where such documents relate to long-term business activities, they shall be kept for the duration of the business relationship and at least eleven years following the end of the year in which the business relationship was terminated.

(4) A credit institution shall store business books for at least eleven years.

Internal audit

Article 183

(1) A credit institution shall organise an internal audit function as a separate organisational unit, functionally and organisationally independent both from the activities it audits and from other organisational units of the credit institution.

(2) By way of derogation from paragraph (1) of this Article, a credit institution may, subject to the prior approval of the Croatian National Bank, entrust the carrying out of internal audits to an audit firm or to one or more persons not employed with the credit institution in question, provided that at least one of these persons meets the criteria referred to in Article 186, paragraph (1) of this Act.

(3) When deciding whether to grant the approval referred to in paragraph (2) of this Article, the Croatian National Bank shall take into account the nature, scale and complexity of services provided by the credit institution.

(4) A credit institution may entrust the carrying out of internal audits to another credit institution which is a member of the same group of credit institutions in the Republic of Croatia, subject to the prior approval of the Croatian National Bank.

Supervision

Article 197

(1) For the purposes of this Act, 'supervision' means verification of whether a credit institution operates in accordance with risk management rules, other provisions of this Act and regulations adopted under this Act, other laws governing the carrying out of financial activities of credit institutions, regulations adopted under these laws, its own rules, and professional standards and rules.

(2) The Croatian National Bank shall exercise supervision of credit institutions by:

1) collecting and analysing reports and information, ongoing monitoring of the operation of credit institutions and other persons required to report to the Croatian National Bank pursuant to this Act and regulations adopted under this Act or other laws and regulations adopted under these laws;

2) carrying out on-site examinations of credit institutions' operation; and

3) imposing supervisory measures.

(3) The Croatian National Bank shall prescribe in detail the conditions and methods of exercising supervision and imposing supervisory measures, as well as obligations of the credit institution's bodies in the course of and following supervision exercised by the Croatian National Bank.

On-site examination

Article 204

(1) A credit institution shall enable authorised persons, at their request, to carry out an on-site examination at the registered office of the credit institution and in other localities in which the credit institution or another person with its authorisation carries out activities and operations subject to the supervision of the Croatian National Bank.

(2) A credit institution shall enable authorised persons, at their request, to carry out an examination of business books, business documentation, and administrative or business records as well as an examination of information and related technologies, to the extent necessary for an individual examination.

(3) A credit institution shall deliver to authorised persons, at their request, computer print-outs, copies of business books, business documentation, and administrative or business records in a paper form or in the form of an electronic record in the medium and format required by the authorised persons. The credit institution shall provide authorised persons with a standard interface providing access to the system for database management used by the credit institution, for the purpose of carrying out an examination supported by computer programmes.

(4) The examination referred to in paragraphs (1) and (2) of this Article shall be carried out by authorised persons during working hours of the credit institution. When necessary because of the scope or nature of the examination, the credit institution shall enable authorised persons to carry out the examination outside its working hours.

Violations related to the obligation of banking secrecy

Article 367

(1) A credit institution that breaches the provisions of this Act on the obligation of banking secrecy shall be fined between HRK 500,000.00 and HRK 1,000,000.00.

(2) A responsible person of the credit institution's management board shall be fined between HRK 25,000.00 and HRK 100,000.00 for the violation referred to in paragraph (1) of this Article.

(3) A legal person shall be fined between HRK 500,000.00 and HRK 1,000,000.00 for the violation referred to in Article 169, paragraph (1) of this Act. A responsible person of that legal person shall be fined between HRK 25,000.00 and HRK 100,000.00 for the violation referred to in Article 169, paragraph (1) of this Act.

(4) A natural person shall be fined between HRK 25,000.00 and HRK 100,000.00 for the violation referred to in Article 169, paragraph (1) of this Act.

(5) The legal person referred to in Article 170, paragraph (1) of this Act who breaches the provisions of this Act on the obligation of banking secrecy shall be fined between HRK 500,000.00 and HRK 1,000,000.00.

(6) A responsible person of the legal person referred to in Article 170, paragraph (1) of this Act shall be shall be fined between HRK 25,000.00 and HRK 100,000.00 for the violation referred to in paragraph (5) of this Article.

(7) The natural person referred to in Article 170, paragraph (2) of this Act who breaches the provisions of this Act on the obligation of banking secrecy shall be fined between HRK 25,000.00 and HRK 100,000.00.

ANNEX XI Payments Systems Act

Granting authorisation to provide payment services

Article 70

(1) The Croatian National Bank shall grant authorisation to provide payment services provided that it assesses from the application referred to in Article 69 of this Act and available information that all of the following conditions are met:

1) in view of the need to ensure the sound and prudent management of the payment institution, the holder of a qualifying holding is suitable, especially with respect to the financial strength and good reputation;

2) the person proposed to be a member of the management board or executive director of the payment institution, where it does not also perform the activities referred to in Article 68, item

(3) of this Act, has a good reputation and the skills and experience required for the provision of payment services;

3) where the payment institution, apart from the provision of payment services, also performs the activities referred to in Article 68, item (3) of this Act, the person responsible for managing operations related to the provision of payment services has a good reputation and the skills and experience required for the provision of payment services;

4) the payment institution is organised in accordance with this Act, that is, the conditions for the operation of a payment institution laid down in this Act or in regulations adopted under this Act are established;

5) the provisions of the Articles of Association or any other relevant legal act of the payment institution comply with the provisions of this Act and regulations adopted under this Act;

6) where it assesses that, in view of the need to ensure the sound and prudent management of the payment institution, this institution has put in place effective and sound governance arrangements comprising a clear management framework with well-defined, transparent and consistent lines of powers and responsibilities, effective procedures for establishing, managing, monitoring and reporting on all the risks to which the payment institution is or might be exposed, and an adequate internal control mechanism, which includes appropriate administrative and accounting procedures, and that the said governance arrangements, internal control mechanism and administrative and accounting procedures are comprehensive and proportionate to the nature, scope and complexity of the payment services provided; and

7) the head office of the payment institution is in the Republic of Croatia.

(2) Prior to granting authorisation to provide payment services, the Croatian National Bank may consult with other competent authorities in order to make a better assessment of the submitted application.

Provision of payment services by payment institutions through agents

Article 76

(1) A payment institution having its registered office in the Republic of Croatia may provide payment services through one or several agents. An agent of a payment institution may be a legal or a natural person in accordance with other regulations.

(2) A payment institution which intends to provide payment services through an agent shall obtain a prior decision to enter the agent into the register from the Croatian National Bank.

(3) A payment institution shall accompany an application for entry into the register referred to in paragraph (2) of this Article with the following:

1) the agent's firm and registered office, or the agent's name and address;

2) a description of the internal control mechanism put in place by the agent to comply with the provisions of the law governing the prevention of money laundering and terrorist financing;

3) for a member of the management board or executive director of the agent which is a legal person, or for the agent who is a natural person, the documentation referred to in Article 69, paragraph (2), item (10) of this Act; and

4) a list of payment services that it intends to provide through agents.

(4) The Croatian National Bank may take all actions necessary, including requiring documentation, to verify the accuracy of the information submitted.

(5) The Croatian National Bank shall refuse to enter an agent into the register where it establishes, based on the documentation and information referred to in paragraphs (3) and (4) of this Article, that:

- the internal control mechanism put in place to comply with the provisions of the law governing the prevention of money laundering and terrorist financing is inadequate, or

- that a member of the management board or executive director of the agent which is a legal person, or an agent who is a natural person, does not have a good reputation or the skills and experience required for the provision of payment services.

(6) An agent may commence work as of the date a decision to enter the agent into the register is adopted.

(7) The Croatian National Bank shall adopt a decision to remove an agent from the register:

1) if a payment institution requests that an agent be removed from the register;

2) if bankruptcy proceedings have been opened against the agent;

3) where the agent is a legal person, upon its removal from the register of companies in the case of a merger, acquisition or division;

4) where the agent is a natural person, upon his/her death;

(8) The Croatian National Bank may adopt a decision to remove an agent from the register:

1) if any of the reasons referred to in paragraph (5) of this Article arise; and

2) if the reason referred to in Article 79, paragraph (8) of this Act arises.

(9) A payment institution may not provide payment services through an agent:

1) as of the date of submission of the decision referred to in paragraph (7), items (1) and (2) of this Article,

2) as of the date of adoption of the decision to open bankruptcy proceedings against the agent;

3) as of the date of removal of the agent from the register of companies in the case of a merger, acquisition or division.

Storing of bookkeeping documents

Article 91

A payment institution shall store bookkeeping documents and other documentation related to this Title in accordance with applicable regulations and professional standards, but for no less than five years.

Supervision of payment institutions

Article 97

(1) The Croatian National Bank shall exercise supervision of payment institutions.

(2) The supervision referred in paragraph (1) of this Article shall mean the verification of whether a payment institution operates in accordance with the provisions of this Act and regulations adopted under this Act, and in relation to its provision of payment services and its activities in accordance with Article 68, items (1) and (2) of this Act.

(3) In establishing the frequency and intensity of the supervision referred in paragraph (1) of this Article, the Croatian National Bank shall take into account the type, scope and complexity of the activities carried out by a payment institution and the risks it is exposed to in its operation.

(4) Other supervisory authorities may also exercise supervision of the operation of payment institutions in accordance with their powers under law, and within their competence.

(5) Where a different supervisory authority is competent for the supervision of a payment institution, the Croatian National Bank may participate in the supervision of that institution with the respective supervisory authority or may require from that supervisory authority the data and information which would be relevant for the supervision of the payment institution in question.

(6) The Croatian National Bank may prescribe in detail the conditions for and the manner of exercising supervision and imposing measures, and the responsibilities of the payment institution's bodies in the course of and following supervision.

(7) Payment institutions shall pay a supervision fee to the Croatian National Bank, whose calculation basis, amount, calculation and payment methods may be prescribed by the Croatian National Bank. The criterion for establishing the amount of the fees may be the type of payment services provided by the payment institution, the minimum own funds that the payment institution is required to maintain, the executed transaction volume or the number of agents through which the payment institution provides payment services.

Register of payment institutions

Article 116

(1) The Croatian National Bank shall maintain a register of payment institutions authorised by it to provide payment services, their branches and agents.

(2) The register shall include, for each entity referred to in paragraph (1) of this Article, a list of payment services which the payment institution is authorised to provide and its registration number. The Croatian National Bank shall update the register on a regular basis.

(3) The register of payment institutions shall be publicly available and accessible on the website of the Croatian National Bank.

(4) The Croatian National Bank shall prescribe the manner of keeping the register.

Violations by other persons

Article 149

(1) A legal or natural person shall be fined between HRK 20,000.00 and HRK 500,000.00:

1) if it provides payment services contrary to the provision of Article 5, paragraph (2) of this Act;

2) if, contrary to the provision of Article 12, paragraph (1) of this Act, it fails to inform the payer of a reduction for the use of a given payment instrument prior to the initiation of a payment transaction;

3) if, in the case referred to in Article 13, paragraph (2) of this Act, it fails to disclose to the payer all charges as well as the exchange rate to be used, prior to the currency conversion;

4) if it, as a payee, levies a charge for the use of a given payment instrument (Article 27, paragraph (6)); or

5) if it provides payment services before it obtains authorisation to provide payment services (Article 65, paragraph (4)).

(2) A responsible person of a legal person shall be fined between HRK 5,000.00 and HRK 50,000.00 for any of the violations referred to in paragraph (1) of this Article.

Violations by payment institutions

Article 151

(1) The payment service provider referred to in Article 5, paragraph (1), item (3) of this Act shall be fined between HRK 20,000.00 and HRK 500,000.00:

1) if it provides payment services through an agent before the agent has been entered into the register or after the agent has been removed from the register (Article 76);

2) if it starts providing payment services in another Member State through a branch contrary to Article 78;

3) if it starts providing payment services in another Member State through an agent contrary to Article 79;

4) if it establishes a branch in a third country without prior authorisation referred to in Article 80, paragraph (2) of this Act;

5) if it fails to notify the Croatian National Bank in accordance with Article 80, paragraph (8) or (9) of this Act;

6) if it fails to ensure that a branch or agent acting on its behalf notifies a payment service user thereof (Article 85);

7) if its own funds are lower than the amount prescribed in Article 86, paragraph (2) of this Act;

8) if it acts contrary to regulations adopted under Article 86, paragraph (3) of this Act;

9) if it fails to safeguard the funds which have been received for the execution of payment transactions in accordance with Article 87 of this Act and subordinate legislation adopted under that Article;

10) if it uses the payment accounts it operates for purposes other than payment transactions (Article 88);

11) if it grants credits connected with the provision of payment services contrary to Article 89, paragraph (1) of this Act;

12) if it provides services referred to in Article 68, item (3) of this Act without keeping separate business books and preparing separate financial statements for payment services (Article 90, paragraph (2));

13) if it fails to store bookkeeping documents and other documentation in accordance with Article 91 of this Act;

14) if it fails to have the financial statements referred to in Article 90 of this Act audited or fails to submit to the Croatian National Bank the reports in accordance with Article 92, paragraphs (1) and (2) of this Act;

15) if it acts contrary to subordinate legislation adopted under Article 93, paragraph (1) of this Act;

16) if it fails to notify the Croatian National Bank of intended outsourcing in accordance with Article 94, paragraph (1) or (2) of this Act;

17) if it outsources its operational activities contrary to the conditions referred to in Article 94, paragraphs (4) to (6) of this Act or contrary to subordinate legislation adopted under paragraph (9) of the same Article of this Act;

18) if it fails to establish and implement governance arrangements in the manner laid down in Article 96, paragraph (1) of this Act, or implements it contrary to subordinate legislation adopted under Article 96, paragraph (2) of this Act;

19) if it acts contrary to subordinate legislation adopted under Article 97, paragraph (6) of this Act;

20) if it fails to enable an authorised person to carry out an on-site examination in the manner and under the conditions prescribed in Article 94, paragraph (6), Article 98 paragraphs (5) and (6) and Article 99 of this Act;

21) if it fails to act in accordance with a decision of the Croatian National Bank;

22) if it fails to report to the Croatian National Bank in accordance with subordinate legislation adopted under Article 111, paragraph (2) of this Act;

23) if it fails to report to the Croatian National Bank on the facts and circumstances referred to in Article 111, paragraphs (3) and (4) of this Act; or

24) if it provides payment services outside the limits of the authorisation issued pursuant to the provisions of this Act (Article 5, paragraph (6)).

(2) A responsible person of the management board of the payment service provider referred to in Article 5, paragraph (1), item (3) of this Act, or, if the payment service provider apart from providing payment services engages in other activities, a director responsible for payment services, shall be fined between HRK 5,000.00 and HRK 50,000.00 for any of the violations referred to in paragraph (1) of this Article.

ANNEX XII Foreign Exchange Act

Prevention of Money Laundering and Foreign Cash Counterfeiting

Article 40

(1) Residents and non-residents shall be obliged, when crossing the state border, to declare to the customs officer any amount of domestic or foreign cash and checks that is being taken into or out of the country that is governed by the act regulating the prevention of money laundering.

(2) The obligation referred to in paragraph 1 of this Article shall also apply to any representative, responsible person or proxy, taking into or out of the country domestic or foreign cash and checks on behalf of any legal person.

(3) The Croatian National Bank shall prescribe the procedures for handling foreign cash suspected of being counterfeit.

Authorised Exchange Offices

Article 46

(1) Exchange transactions conducted by authorised exchange offices shall comprise the purchase of foreign cash and checks denominated in a foreign currency and the sale of foreign cash in exchange for kuna cash.

Article 69

(1) A fine of HRK 5,000.00 to HRK 50,000.00 shall be imposed for misdemeanor on any domestic and foreign natural person, domestic and foreign legal person, representative, responsible person or proxy of any domestic or foreign legal person, who attempts to take or takes over the state borders, without declaring it to the customs officer, cash and checks in the amounts governed by the act on the prevention of money laundering.

(2) Cash and checks, as the subjects of misdemeanors referred to in paragraph 1 of this Article, shall be seized on the basis of a misdemeanor ruling in favour of the Government Budget of the Republic of Croatia.

(3) Cash and checks, as the subjects of misdemeanors, may be seized even when they are not the property of the person committing the misdemeanor.

(4) By way of exception, in especially warranted situations under especially extenuating circumstances, the body in charge of misdemeanor proceedings may decide that cash and checks, as the subjects of misdemeanors referred to in paragraph 1 of this Article, are not to be seized or to be seized only in part.

Article 70

When performing foreign exchange control, the Foreign Exchange Inspectorate and the customs authority, shall temporarily seize the domestic and foreign cash and the documentation and other objects which are used to commit the misdemeanor, which result from the misdemeanor or which may be used as evidence in misdemeanor proceedings, in accordance with the regulations governing such misdemeanor proceedings and they shall issue a receipt for any domestic or foreign cash, documentation or other objects seized. The domestic and foreign cash shall be paid immediately into special accounts with the Foreign Exchange Inspectorate of the Ministry of Finance.

Article 74

(1) The Foreign Exchange Inspectorate of the Republic of Croatia shall conduct misdemeanor proceedings of the first instance.

(2) An appeal may be filed with the High Magistrate Court of the Republic of Croatia against the ruling of the Foreign Exchange Inspectorate of the Republic of Croatia.

ANNEX XIII Capital Market Act

Management board of an investment firm

Article 21

(1) An investment firm shall have at least two members of the management board who effectively direct the business and jointly represent the investment firm. One member of the management board shall be appointed as the president of the management board.

(2) By way of derogation from paragraph 1 of this Article, the management board of an investment firm which is not authorised to hold money and financial instruments of their clients may have one member only. In that case, investment firm shall establish additional measures and procedures that will ensure sound and prudent management of the investment firm. If that investment firm has more members of the management board, paragraph 1. of this Article shall apply analogously.

(3) Members of the management board direct the business and jointly represent the investment firm, unless the foundation act of investment firm prescribes otherwise.

(4) The members of the management board of the investment firm must be of sufficiently good repute and must have the required professional qualifications and be sufficiently experienced so as to ensure the sound and prudent management of the investment firm.

(5) The members of the management board of the investment firm shall direct the business of the investment firm on a full-time basis and on the basis of employment with the investment firm.

(6) At least one member of the management board must be fluent in Croatian.

(7) The members of the management board of the investment firm shall direct the business of the investment firm from the territory of the Republic of Croatia.

(8) Management board of the investment firm may authorise a person with special purpose power of attorney (prokurist) to direct the business of the investment firm or to conclude the contract and carry out legal actions on behalf and for the account of the investment firm, jointly with at least one member of the management board of the investment firm.

(9) Accompany with the entrance of the person with special purpose power of attorney (prokurist) in the court register, management board of the investment firm shall enter all limitations of that special purpose power of attorney (prokura).

(10) Requirements that has to fulfil the person to whom the special commercial proxy (prokura) is given, means and modes of granting the special commercial proxy, the scope of the authority, including all limits in undertaking certain actions by special commercial proxy, shall be determined by the foundation act of investment firm.

(11) In the case that the investment firm is managed by the board of directors, the board shall appoint at least two executive directors. The provisions of this Act and the regulations adopted on the basis of this Act relating to the members of the management board of the investment firm shall apply analogously to executive directors.

By virtue of an ordinance, the Agency shall specify in more detail the requirements which must be met by the members of the management board of the investment firm, as well as the contents of the application for issuance of approval for the position of a member of the management board, the documents that must accompany the application and the contents of the documents.

Keeping of business records

Article 41

(1) An investment firm shall keep and preserve records of all investment services and activities, as well as transactions undertaken by it in such a manner as to enable supervision of the business in accordance with Article 37 of this Act, and in particular to ascertain that the investment firm has complied with all obligations with respect to clients and potential clients.

(2) An investment firm shall organise its operations and keep orderly business documents and other administrative and business records in a way that it is possible at any time to check the course of a transaction it has made for its own account or for a client's account.

(3) An investment firm shall keep all records documenting the transactions in respect of each individual client separate from the records concerning transactions in respect of other clients and from the records concerning its own operations.

(4) An investment firm shall protect all business records from unauthorised access and possible loss of records, and preserve in a way that ensures durability of records.

(5) An investment firm shall preserve, for a minimum period of 5 years from the end of the year in which a transaction is entered into, all records and information on all transactions in financial instruments which it makes for either its own account or for a client's account.

In the case of branches of investment firms from another Member State the obligation laid down in this Article with regard to transactions undertaken by the branch shall apply.

Article 50

(1) In assessing the application referred to in Article 44, paragraph 1, and the information referred to in Article 49, paragraphs 1, 2 and 3, in order to ensure the sound and prudent management of the investment firm in which an acquisition is proposed, and having regard to the likely influence of the proposed acquirer on the investment firm, the Agency shall appraise the suitability of the proposed acquirer and the financial soundness of the proposed acquisition against all of the following criteria:

1. the reputation of the proposed acquirer;
2. the reputation and experience of any person who will direct the business of the investment firm as a result of the proposed acquisition;
3. the financial soundness of the proposed acquirer, in particular in relation to the type of business pursued in the investment firm in which the acquisition of a qualifying holding is proposed;
4. whether the investment firm will be able to comply and continue to comply with the requirements of this Act and other legislation, where applicable, on an individual and consolidated basis, in particular, whether the group of which the investment firm will become a part has a structure that makes it possible to exercise effective supervision, effectively exchange information among the competent authorities, and whether it is possible to determine the allocation of responsibilities among the competent authorities;
5. whether there are reasonable grounds to suspect that, in connection with the proposed acquisition, money laundering or terrorist financing, within the meaning of the regulations governing money laundering and terrorist financing, has been committed or attempted, or could be committed.

(2)The Agency may oppose the proposed acquisition only if the requirements of paragraph 1 of this Article are not met or if the information provided by the proposed acquirer is incomplete.

(3) The documents required for the assessment, which must be submitted to the Agency with the application referred to in Article 44, paragraph 1, shall be proportionate and adapted to the nature of the proposed acquirer and the proposed acquisition.

(4) The Agency shall specify, by virtue of an ordinance, a list of the documents referred to in paragraph 3 of this Article.

(5) Where two or more proposals to acquire or increase qualifying holdings in the same investment firm have been notified to the Agency, the latter shall treat the proposed acquirers in a non-discriminatory manner.

(6) If an investment firm becomes aware of an acquisition or disposal of a qualifying holding in the investment firm which would exceed or fall below 20%, 30% or 50%, it shall notify the Agency without delay.

(7) Once a year, an investment firm shall submit to the Agency, by 31 March of the current year, a list of names of all shareholders and members possessing holdings or qualifying holdings and the sizes of such holdings as at 1 January of the current year.

Conduct of business obligations when providing investment services to clients

Article 54

(1) When providing investment services and/or, where appropriate, ancillary services to clients, an investment firm shall act in accordance with the best interest of its clients, fairly and professionally and comply with the provisions of this Act.

(2) The members of the management board, supervisory board, brokers, investment advisers, other employees of the investment firm and tied agents shall safeguard the information on the clients, the balance and transactions in the clients' accounts, the services they provide to the clients, as well as other information and facts they learn in connection with the provision of the investment services and, where appropriate, ancillary services. Such information shall be regarded as confidential and the persons referred to in this paragraph shall neither use them or disclose to third parties nor enable third parties to use them.

(3) The information referred to in paragraph 2 of this Article shall not be treated as confidential when such information is requested by the Agency, stock exchange, judicial and administrative bodies in exercise of their supervisory and other public authorities in accordance with this Act or another act, or when clients authorise disclosure of such information.

Agency's competence for the operation of investment firms

Article 247

(1) The Agency is competent for supervision of the operation of investment firms with registered office in the Republic of Croatia, as regards any investment services and activities provided and performed by them in and outside the territory of the Republic of Croatia, and for the supervision, on a consolidated basis, of groups of investment firm in the Republic of Croatia.

(2) For the purpose of paragraph 1 of this Article, supervision means an inspection in order to establish whether the investment firm subject to supervision operates in accordance with the provisions of this Act, ordinances adopted pursuant to it, as well as in accordance with its own rules, standards and the codes of conducts, in a manner that enables an orderly operation of the capital market and the implementation of measures and activities aimed at eliminating the established violations and irregularities.

(3) Where in the opinion of the Agency it is necessary to perform the supervision provided for in paragraph 1 of this Article, the Agency is authorised, in accordance with this Act and other regulations, to require from the following persons to submit reports and information, carry out a review of its account books and business documentation with:
1. a person that is closely related to the investment firm,
2. a person to which the investment firm has outsourced critical and important business functions,
3. a shareholder of a qualifying holding in the investment firm.

(4) Where another supervisory body is competent for supervising the person referred to in paragraph 4 of this Article, the Agency will review the account books and business documentation of that person in co-operation with that body, in accordance with Part 6 Title 2 of this Act.

(5) The operation of credit institutions concerning provision of investment services and the performance of activities is supervised independently by the Agency or in co-operation with the Croatian National Bank.

(6) When exercising the supervision referred to in paragraph 5 of this Article, the Agency may order a credit institution supervisory measures referred to in Articles 257 - 261 hereof, as well as specific supervisory measures referred to in Article 262.

(7) Where a credit institution fails to act in accordance with the Agency's decision requesting from it to eliminate the established violations and irregularities, the Agency shall inform thereof the Croatian National Bank without delay, and shall withdraw the prior approval. From the moment when the decision on the withdrawal of preliminary consent is delivered, the credit institution shall not perform any investment services and activities and related ancillary services to which the above mentioned consent related.

(8) The provisions of Article 16 and paragraphs 5 - 7 of this Article of the Act shall not apply to credit institutions in the event when the provisions of Article 9 hereof apply to the same institutions.

Subject of supervision

Article 254

(1) When carrying out supervision the Agency shall particularly:

1. review the organisational conditions, strategies, policies and procedures that the investment firm has set up in order to comply with the provisions of this Act and regulations adopted pursuant to this Act.

2. evaluate the financial position and risks to which the investment firm is exposed or to which it may be exposed in its operation.

(2) Pursuant to reviews and evaluations referred to in paragraph 1 of this Article, the Agency shall establish whether the investment firm has put in place a suitable organisational structure, strategies, policies, procedures and capital that ensure a management system and coverage of the risks it is exposed to or to which it may be exposed in its operation.

(3) In determining the frequency and intensity of exercising reviews and evaluations referred to in paragraph 1 of this Article, for each investment firm, the Agency shall take into account the size and importance of the investment firm within the capital market of the Republic of Croatia, and the nature, scale and complexity of investment services and activities and related ancillary services performed by the investment firm.

(4) The reviews and evaluations referred to in paragraph 1 of this Article are performed by the Agency at least on an annual basis for each investment firm.

ANNEX XIV Insurance Act

Approval to acquire qualifying holding

Article 21

(1) The acquisition of shares in an insurance undertaking, whereby a person directly or indirectly acquires a holding equalling or exceeding the qualifying holding (hereinafter: holder of qualifying holding) in the insurance undertaking shall be subject to the approval of the supervisory authorities (hereinafter: approval to acquire qualifying holding).

(2) In the event of any further acquisition of shares in an insurance undertaking, whereby the person who has qualifying holding would increase his holding so that the proportion of the voting rights or of the capital he holds would reach or exceed 20%, 33% or 50% or so that the insurance undertaking would become his subsidiary, he shall obtain approval from the supervisory authorities.

(3) Where the person which has been granted the approval referred to in paragraphs 1 or 2 of this Article intends to dispose of his shares, which would result in the holding being reduced below the threshold for which the approval was granted, the person in question must inform the supervisory authorities thereof.

(4) The supervisory authorities shall prior to issue of the approval for acquisition of a qualifying holding or the holding referred in paragraph 2 of this Article notify the competent supervisory authorities of the concerned Member State if the entity possessing qualifying holding is one of the following entities:

1. an insurance undertaking, bank or stock-broking company which has been granted approval for carrying out insurance operations, banking operations or transactions with securities,

2. controlling undertaking of an insurance undertaking, bank or stock-broking company referred to in point 1 of this paragraph,

3. an entity under management of the same entity or entities managing the insurance undertaking, bank or stock-broking company referred to in point 1 of this paragraph.

(5) The supervisory authorities shall notify and exchange information with the competent supervisory authorities of the Member State concerned on the eligibility of the acquirer of qualifying holding or the holding referred to in paragraph 2 of this Article.

(6) The supervisory authorities shall specify the method of notification referred to in paragraph 3 of this Article.

(7) The approval referred to in paragraphs 1 and 2 of this Article shall become invalid if the entity, within six months of the date of issue by the supervisory authorities of a decision to grant approval, fails to acquire the shares to which the approval relates.

Requirements for the position of a member of the board of directors

Article 27

(1) The position of the member of the board of directors of an insurance undertaking may be assumed by any person meeting the following requirements:

- the candidate has a university degree;

- the candidate has adequate professional qualifications, competence and experience needed to manage the operations of an insurance undertaking in a sound and prudent manner;

- the candidate has never held a managing position in an undertaking or any other financial institution or company against which bankruptcy proceedings have been instituted or in respect of which the authorisation to conduct business has been revoked;

- the candidate meets the requirements for the position of the member of the board of directors laid down in the Companies Act;

- the candidate is not member of a board of directors or procurator of another company.

(2) The professional qualifications and experience referred to in paragraph 1, second subparagraph of this Article shall mean experience of at least three years in managerial positions in an insurance undertaking or six years' working experience on matters familiar to insurance undertaking business.

Application for issue of authorisation to carry on insurance business

Article 59

(1) An application for a authorisation required to carry on insurance business shall be accompanied by:

1. a scheme of operations;

2. Articles of association of the insurance undertaking in the form of an authenticated notary public's document;

3. a list of shareholders including personal information about them, name of the undertaking and its principal place of business, the total nominal value of shares held and the amount of respective holdings, expressed as percentage, in the share capital of the insurance undertaking;

4. the shareholders – legal persons which are holders of qualifying holdings shall submit as follows:

- an extract from the judicial register of companies or another equivalent public register;

- where the shareholder is a joint-stock undertaking, in addition to the abovementioned, an extract relating to the shareholder in question from the shareholders' register or, in the case of bearer shares, an authenticated transcript of the notary public's document showing the list of the persons present at the last general meeting of shareholders; where the shareholders are foreign legal persons, notarised translation of the concerned documents must be submitted;

- financial statements for the past two financial years;

5. a list of persons related to the holders of qualifying holdings along with the description of their relationship;

6. contracts on outsourced business if the insurance undertaking intends to authorise other persons to carry on certain operations.

(2) An application for issue of authorisation to carry on insurance business shall be accompanied by an opinion of a certified actuary on whether the insurance undertaking will be able to meet the capital adequacy requirements given the nature and volume of the business to be carried on.

Confidential data

Article 137

(1) An insurance undertaking shall be obliged to treat as confidential all data, information, facts and circumstances that they have received or become aware of in the course of operations with a certain insurance undertaking or the policyholder or the insured or any other person asserting the rights under an insurance contract.

Obligation to protect confidential data

Article 138

(1) Members of the insurance undertaking's bodies, its shareholders, employees and other persons who, in their work or provision of services for the insurance undertaking, have access to the data referred to in Article 137 of this Act may not disclose these data to third parties, use them against the interests of the insurance undertaking and its clients or enable third parties to use them.

(2) The obligation to protect personal data shall not apply in the following cases:

1. if a party agrees expressly and in writing that certain confidential data may be disclosed;

2. if the information is required to establish the facts in criminal proceedings and if presentation of this information is required or ordered in writing by the competent court;

3. in the cases provided by the Act on the Prevention of Money Laundering;

4. if such information is required to determine the legal relationship between an insurance undertaking and a policyholder or an insured person or other person asserting the rights under an insurance contract in the course of legal proceedings;

5. if such information is required in inheritance proceedings and if disclosure of this information is required or ordered in writing by the competent court;

6. if such information is required for the purpose of a seizure of property of a policyholder or other person asserting the rights under an insurance contract, and if disclosure of this information is required or ordered in writing by the competent court;

7. if such information is required by the supervisory authority or another supervisory body for the purpose of supervision carried out within the framework of itscompetences;

8. if such information is required by a tax authority in proceedings carried out by the latter within the framework of its competences;

9. in the cases provided by the Act on Compulsory Insurances in Transportation.

(3) The obligation to protect confidential data shall also apply to the persons referred to in paragraph 1 of this Article after they leave the insurance undertaking or after they cease to be shareholders or members of the bodies of the insurance undertaking.

(4) The supervisory authority or other authorities or bodies and courts shall be allowed to use the information gathered pursuant to paragraph 2 of this Article solely for the purposes for which these have been gathered.

Gathering, keeping and using personal data

Article 139

(1) Insurance undertakings and the Croatian Insurance Bureau shall gather, process, keep, submit and use personal data which are necessary for underwriting policies and for settling claims arising from any insurance pursuant to this Act and in accordance with the Personal Data Protection Act and other regulations relating to data protection.

(2) Insurance undertakings and the Croatian Insurance Bureau may establish, maintain and keep the following databases:

1. database of the insured persons;

2. database of loss events;

3. database for the assessment of insurance covers and loss compensation amounts.

Method of supervision

Article 157

(1) The supervisory authority shall exercise the supervision of insurance undertakings by way of:

1. monitoring, collecting and verifying reports and notifications submitted by insurance undertakings and other persons that are obliged, in accordance with the provisions of this Act and other laws, to report to the supervisory authority or notify it of particular facts and circumstances;

2. carrying out examinations of operations of insurance undertakings;

3. imposing supervisory measures in compliance with this Act.

ANNEX XV Act on Croatian Financial Services Supervisory Agency

Chapter I

General Provisions

Article 1

This Act regulates:

- the legal position of the Croatian Agency for Supervision of Financial Services (hereinafter: "the Agency")
- its internal structure and organisation
- conditions for the appointment, period of office and discharge of the President and members of the Board of the Agency
- decision making
- the duty for the preservation of confidentiality and liability,
- conditions for the appointment, period of office and the functions of the Council of the Agency
- the objectives, scope of activities and competence of the Agency and
- its financing and reporting.

Article 2

The terms in this Act have the following meanings:

1) **the Agency** means the Croatian Agency for Supervision of Financial Services,

2) **the supervised entities** all the legal and natural entities that deal with the provision of financial services, financial market advising, sales, brokerage activities or asset management for users of financial services,

3) **the supervisory body** the Croatian Agency for Supervision of Financial Services the **scope of activities** and competence of which includes supervision of the financial market, supervised entities and the financial services they provide,

4) **the Council** is the advisory body of the Agency,

5) **financial services** all the services provided by the supervised entities

6) **the financial market** established places or computer networks meant for trading financial instruments,

7) the **Croatian Securities Exchange Commission** is the legal entity that concerns itself with matters of supervision of stock exchanges and regulated public markets operations, authorised companies and issuers of securities, investment management companies and privatisation investment funds, investment and privatisation investment funds, the Croatian Defenders of the Homeland War and Members of their Families Fund, brokerage companies, brokers and investment advisors, institutional investors and the Central Depositary Agency,

8) **Agency for Supervision of Pension Funds and Insurance** is the legal entity that concerns itself with supervision of the operation so the pensions companies, the pensions funds, the pensions insurance companies and the Central Insured Persons Register,

9) the **Directorate for Supervision of Insurance Companies** is the legal entity that carries out supervision of the operations of insurance companies, insurance representatives and insurance agents.

CHAPTER II

THE CROATIAN AGENCY FOR SUPERVISION OF FINANCIAL SERVICES

Legal position

Article 3

(1) The Agency shall be an independent legal person with public authorities within its scope of activities and competence prescribed by this and other acts, and is responsible to the Croatian Parliament.

(2) The headquarters of the Agency is in Zagreb.

(3) The internal structure and operations of the Agency are regulated by the Statutes, which is the fundamental constitutive act of the Agency. The Statutes shall be adopted by the Agency and confirmed by the Croatian Parliament.

(4) The by-laws laying down the internal organisational structure, the conditions for employment and the work of employees in accordance with the Labour Act, shall be adopted by the Agency.

The internal structure and organisation of the Agency

Article 4

(1) The Agency shall have a Board consisting of five members, one of whom is the President.

(2) The President and members of the Board shall be appointed and discharged by the Croatian Parliament at the recommendation of the Government of the Republic of Croatia.

(3) The President of the Board of the Agency shall represent the Agency and manage its activities.

(4) The President of the Board of the Agency shall appoint a deputy from among the other members.

Conditions for appointment, duration of office and discharge of the President and members of the Board of the Agency

Article 5

(1) To be appointed the President or a member of the Board of the Agency, a person must be a citizen of the Republic of Croatia, have a degree-level education, appropriate professional knowledge and work experience in the area of finance, accountancy, business management, actuarial science or law, making the person capable and worthy to be a member.

(2) The President and the members of the Board of the Agency shall be appointed for a period of 6 (six) years from the day of appointment and are eligible for reappointment.

(3) The President and members of the Board shall carry out their duties in the Agency on a professional basis.

(4) The President and members of the Board of the Agency are bound to behave in a manner not diminishing their personal reputation or the reputation of the Agency and not to impugn their independence in the performance of their office or the independence of the Agency.

(5) Any form of influence on the Agency's activities that might impugn its legally prescribed independence is forbidden**.**

Article 6

(1) While performing their offices, the President and members of the Board of the Agency are entitled to remuneration and other material rights in accordance with the by-laws of the Agency.

(2) The President and members of the Board of the Agency are entitled to publish professional and scientific papers and to participate in activities of professional or scientific meetings.

(3) The President and members of the Board of the Agency during their period of office and the employees in the administrative and professional services of the Agency must not accept any compensation, position or employment or provide services with respect to:

- supervised entities and

- persons who are deemed to be connected with these entities by the laws that govern such connections.

(4) Persons as defined in Paragraph 3 of this Article must not have shares or ownership shares in insurance companies, legal entities performing brokerage activities in insurance, investment fund management companies, pension fund management companies, pension insurance companies, brokerage companies and authorised companies, legal entitles performing leasing and factoring operations and entities linked with them.

(5) The President and members of the Board of the Agency cannot be persons who are members of the Croatian Parliament, who perform some other duty to which they have been appointed by the Parliament or the Government of the Republic of Croatia, cannot be a member of the Government of the Republic of Croatia and cannot be a person who performs some office in bodies of local and regional self-government and in the bodies of political parties and union organisations.

(6) In order to prevent the conflict of interest of the President and members of the Board of the Agency and employs with respect to supervised entities and entities connected wit them, the Agency will adopt a special Code of Conduct.

(7) The information that the President and members of the Board of the Agency and employees come into possession of during the performance of their duties and work must not be used in any way for the acquisition of material gain.

(8) Persons as defined in Paragraph 3 of this Article must not in a period of one year of the cessation of the performance of their office or employment in the Agency accept any memberships in the management boards or Supervisory Board of supervised entities or entities connected with them.

(9) The President and members of the Board of the Agency have the right to remuneration equivalent to the last salary paid in the month before their discharge until they are re-employed, but at the most for one year from the day of the cessation of the performance of their office.

Article 7

(1) The Croatian Parliament may discharge the President and members of the Board of the Agency before the end of their period of office at the recommendation of the Government of the Republic of Croatia in the following cases:

- if the person himself or herself requests to be discharged,
- if after the appointment any of the circumstances described in Article 6 Paragraphs 3, 4, and 5 should occur,
- if the person should permanently lose the ability to perform the office,
- if the person is sentenced with legal effect to a term of imprisonment,
- if the person is in breach of the obligation to preserve confidentiality in the performance of his or her office and
- if the person performs a duty or activities which are incompatible with the office of a member of the Board of the Agency or if by unconscientious or improper work the person causes the Agency major damage or major damage to the Agency and operations of the Agency.

(2 The Agency is obliged to inform the Government of the Republic of Croatia of any reason for the discharge of the President or a member of the Board of the Agency before the ending of the period of office.

(3) Before a decision is made to discharge the President or a member of the Board of the Agency, such persons must be allowed to make a statement on the reasons for their discharge.

(4) In cases referred under Paragraph 1 of this Article, except in the case of permanently loosing the ability to perform the office, the provision of Article 6 Paragraph 9 of this Act, shall not be applied.

Decision making

Article 8

(1) All decisions from the scope of activities and competence of the Agency shall be made by the Board at sessions with a majority of at least three votes with the proviso that a member of the Board or the President may not abstain from voting.

(2) Three members of the Board of the Agency shall constitute a quorum necessary for the making of decisions and yet at every session of the Board of the Agency the President must be present, or in the absence of the President, the deputy President must be present. (3) Before entering into force the by-laws of the Agency will be published in the Official Gazette of the Republic of Croatia. All individual acts of the Agency that determine the someone's rights or obligations must be published after they become final in the Official Gazette of the Republic of Croatia.

(4) If the Agency considers that the publication of some individual act would not essentially affect the interests of financial services users such an instrument need not be published or only the pronouncement of it may be published.

The duty to preserve confidentiality

Article 9

(1) The President and members of the Board of the Agency and its employees are bound to preserve the confidentiality of documents and data that they learn of in the performance of their duties and activities, the communication of which to an unauthorised person would harm the reputation and interests of the Agency.

(2) The duty to preserve confidentiality endures even after the cessation of membership in the Board or of employment in the Agency.

Liability

Article 10

The President and members of the Board of the Agency and employees in the Agency are not liable for damage that arises during the performance of their duties in the context of their competence and the laws that they enforce, unless it is proven that they performed or omitted to perform a certain action from which harmful consequences arose either deliberately or with gross negligence.

CHAPTER III

The Council of the Agency

Conditions for appointment and period of office

Article 11

(1) The Agency shall have a Council.

(2) The Council shall be an advisory body of the Agency and shall consist of nine members, three of whom shall be appointed by the Government of the Republic of Croatia and the other five shall be appointed by the representatives of associations of supervised entities at the Croatian Chamber of Commerce, while the President of the Board of the Agency shall be a member ex officio.

(3) A member of the Council must have degree level qualifications, and a reputation of an expert in the area of finance, accountancy, management, actuarial science or law.

(4) The period of office of members of the Council is four years and members are eligible for re-election to the Council. If some member of the Council ceases to perform the duty before the end of the period of office, another person shall be elected to that member's place under the same conditions until the end of the period of office of the member instead of whom the person is appointed.

(5) The material rights of Council members shall be determined by the Statutes and the other by-laws of the Agency.

(6) Bodies as defined in Paragraph 2 of this Article shall discharge a member of the Council of the Agency before the end of the period of office:

- if he requests to be discharged himself, and
- in the event a person is sentenced with legal effect to a term of imprisonment.

The President of the Board of the Agency shall be discharged of the membership in Council in the event of the occurrence of any of the circumstances as defined in Article 7 of this Act.

The function of the Council of the Agency

Article 12

The Council of the Agency gives its opinions and professional and scientific advice for the sake of the development of the supervisory practice.

CHAPTER IV

THE OBJECTIVES, PRINCIPLES, SCOPE OF ACTIVITIES AND COMPETENCE OF THE AGENCY

Objectives

Article 13

The fundamental objectives of the Agency are:

- promotion and preservation of the stability of the financial system and
- supervision of legality of the supervised entities operations.

Principles

Article 14

(1) In the achievement of its objectives as defined in Article 13 of this Act the Agency shall be governed by the principles of:

- transparency,
- the confidence among participants of the financial markets and
- reporting to consumers.

(2) The Agency shall acquaint the public with the role and manner of functioning of the financial system, including the development of awareness of the benefits and risks that are connected with various types of investments and financial activities.

(3) The Agency shall provide a rapid and economical approach to all kinds of information that might be useful to financial services users, investors and the rest of the public.

(4) The Agency shall concern itself with matters as defined in Paragraph 2 and 3 of this Article with attention to the amount of the costs of regulation of the supervised entities.

Scope of activities and competence

Article 15

In the performance of its public authorities, the Agency is authorised to:

1) adopt regulations on enforcement of this Act, the Securities Market Act, the Investment Funds Act, the Privatisation Investment Funds Act, the Act on the Takeover of Joint- Stock Companies, the Act on the Fund of Croatian Defenders from the Homeland War and Members of their Families, the Retired persons' Fund Act, the Act on Compulsory and Voluntary pension Funds, the Act on Pension Insurance Companies and Payment of Pension Annuities on the Basis of Individual Capitalised Savings, the Insurance Act, the Insurance Brokerage and Representation Act and other acts when it is authorised by law.

2) exercise supervision over the operations of:

- stock exchanges and regulated public markets, authorised securities companies and issuers,
- companies for the management of investment, privatisation investment and pension funds, investment funds, privatisation investment funds, pension funds, Fund of the Croatian Defenders of the Homeland War and Members of their Families, and the Retired Persons' Fund,
- brokerage companies, brokers and investment advisers,
- institutional investors,
- the Central Depositary Agency
- insurance companies, pension insurance companies, insurance brokers and representatives;
- legal entities performing the operations of leasing and factoring, unless the banks perform them within the scope of their registered activities,

all in compliance with this Act and the by-laws regulating the subject matter.

3) order measures for the obviation of unlawfulness and irregularity that have been established.

4) issue and to withdraw:

- permissions, authorisations and consents when it is authorised to do this by the Securities Market Act, the Investment Funds Act, the Privatisation Investment Funds Act, the Act on the Fund of Croatian Defenders of the Homeland War and Members of their Families, the Retired persons' Fund Act and the Act on the Takeover of Joint- Stock Companies,
- licenses, authorisations, approvals and consents when authorised pursuant to the Act on Compulsory and Voluntary pension Funds, the Act on Pension Insurance Companies and Payment of Pension Annuities on the Basis of Individual Capitalised Savings and
- approval and consents when authorised to do so pursuant to Insurance Act, the Insurance Brokerage and Representation Act, the Regulations on conditions to obtain authorisation for performing actuarial activities and the Regulations on the conditions for obtaining authorisation for performing representation and brokerage activities.

5) encourage, organise and supervise measures for the effective functioning of the financial markets.

6) keep books and registers in accordance with this Act and the acts mentioned in Paragraph 1 of this Article.

7) launch initiatives for the adoption of laws and other regulations and to inform the public of the principles according to which the financial market operates.

8) adopt by-laws in order to prescribe the conditions, manner and procedures for performing unified supervision within its scope and authority.

9) To give opinions on the enforcement of this Act and the separate acts as defined in Paragraph 1 of this Article at the request of parties in a procedure or parties having the proved legal interest in the procedure.

10) undertake other measures and perform other activities in compliance with the legal authorities

11) report to other supervisory, administrative and judicial bodies on all issues that directly or indirectly impinge on their scope of activities and competence, as occasioned by proceedings that are being handled in front of these bodies and that are connected with procedures from the scope of activities and competence of the Agency.

Article 16

(1) The Agency and the Croatian National Bank (hereinafter: CNB) must at mutual request supply each other with all data and information about supervised entities from their scope of activities and

competence, which are necessary in the procedure of exercising supervision and in a procedure related to the issuance of authorisations.

(2) The supervisory bodies as defined in Paragraph 1 of this Article must mutually inform each other on irregularities that they learn of during the exercise of supervision, if these findings are important for the activities of the other supervisory body.

(3) Exchange of data and information in compliance with this Article shall not be considered breach of confidentiality, while the Agency the CNB are bound to keep the confidentiality of data and information and can use them only for the purposes for which they were supplied.

(4) The extent of exchange of information and the coordination of procedures and activities at supervision and regulation of financial institutions and groups shall be determined by a mutual agreement on collaboration between the Agency and the CNB.

Article 17

In the execution of the statutorily defined objectives and tasks, the Agency shall collaborate with the Government of the Republic of Croatia and other bodies of government and in the framework of its competence shall take measures to improve this collaboration.

Article 18

(1) The Agency may be a member of international organisations competent for the area of the supervision of financial institutions and markets.

(2) The Agency shall collaborate and exchange information arising from the supervision of the operations of supervised entities as defined in Article 14 Paragraph 2 with similar foreign institutions that exercise supervision of financial institutions and markets.

Article 19

(1) At procedures undertaken by the Agency within its competence, the provisions of the General Administrative Procedure Act will be applied, unless otherwise prescribed by law.

(2) The acts of the Agency are final and an administrative action can be filed against them.

CHAPTER V

FINANCING AND REPORTING

Financing

Article 20

(1) The Agency shall be financed:

- by the state budget funds,
- from fees from the assets and revenue of supervised entities and
- from fees for services from the scope of activities of the Agency provided.

(2) The Agency is obliged to prepare for each calendar year a plan of revenue and expenditure and submit it to the Ministry of finance.

(3) For the financing of the Agency as defined in Paragraph 2 subparagraph 2 of this Article, the highest charge may amount 0,8 o/oo (the thousandth part) with the proviso that the Agency shall by special Regulations for each year determine the calculation and amount of the fee, and the manner and execution of the collection of the *fee*.

(4) Administrative fees collected by the Agency shall be paid in favor of the state budget of the Republic of Croatia.

(5) Grants or donations received by the Agency from bodies or funds of the European Union for the advancement of its professional or technical level of activity do not form part of the annual plan of revenue and expenditure of the Agency.

(6) In the event that the fee collected in the total revenue of the Agency exceeds expenditure, the surplus of funds shall constitute the revenue of the subsequent calendar year.

(7) In the event that collected fee in the total revenue is not sufficient to cover expenditure, the shortage of funds shall be made up from the planned revenue of the state budget.

Reporting

Article 21

The Agency is obliged once a year, for the preceding calendar year, to submit to the Government of the Republic of Croatia and to the Croatian Parliament, a report on its activities and on the state of affairs of financial institutions and markets that fall within its scope of activities and competence.

CHAPTER VI

PENALTY PROVISIONS

Article 22

(1) Offences as prescribed by the Securities Market Act (Official Gazette no. 84/02), the Investment Funds Act (Official Gazette, no. 107/95, 12/96 and 114/01), the Privatisation Investment Funds Act (Official Gazette no. 109/97 and 114/01), Act on the Takeover of Joint- Stock Companies (Official Gazette, no. 84/02 109/02), Act on Compulsory and Voluntary pension Funds (Official Gazette no. 49/99, 63/00, 103/03 and 117/04), the Act on Pension Insurance Companies and Payment of Pension Annuities on the Basis of Individual Capitalised Savings (Official Gazette no. 106./99 and 63/00), the Insurance Act (Official Gazette no. 9/04, 20/97, 47/97 revised wording,116/99 and 11/02) and the Insurance Brokerage and Representation Act (Official Gazette, no 27/99) fall under the statute of limitations as follows:

- for the filing of an offence proceeding [for an indictment], within a period of 3 years from the day the offence was committed,
- for the execution of sanctions that have been imposed, in a period of 2 years from the day the ruling becomes legally valid.

(2) The application of the statute of limitations is interrupted by every action by a competent body but ensue in every case when twice the time from the time provided for in Paragraph 1 of this Article has elapsed.

CHAPTER VII

TRANSITIONAL AND FINAL PROVISIONS

Article 23

In the Securities Market Act (Official Gazette no. 84/02), the Investment Funds Act (Official Gazette, no. 107/95, 12/96 and 114/01), the Privatisation Investment Funds Act (Official Gazette no. 109/97 and 114/01), Act on the Takeover of Joint- Stock Companies (Official Gazette, no. 84/02, 87/02 and 120/01), the Act on the Fund of Croatian Defenders of the Homeland War and Members of their Families (Official Gazette no. 163/03 and 112/04), the Retired persons' Fund Act (Official Gazette no. 93/05), the Act on Compulsory and Voluntary pension Funds (Official Gazette, no. 49/99, 63/00, 103/03 and 117/04),), the Act on Pension Insurance Companies and Payment of Pension Annuities on the Basis of Individual Capitalised Savings (Official Gazette, no. 106/99 and 63/00), the Insurance Act (Official Gazette no. 9/94,20/97, 46/97 revised wording, 116/99 and 11/02), the Insurance Brokerage and Representation Act (Official Gazette no. 27/99) , in other acts and in all by-law regulations, the names of the Croatian Securities Exchange Commission, the Agency for Supervision of Pension Funds and Insurance and the Directorate for Supervision of Insurance Companies are

replaced in the appropriate gender, number and case with the name of the Croatian Agency for Supervision of Financial Services.

Article 24

(1) The Government of the Republic of Croatia will, at latest within 15 days from the enforcement of this Act, recommend to the Croatian Parliament the appointment of the President and members of the Board of the Agency.

(2) Bodies authorised for appointment as defined in Article 11 Paragraph 2 of this Act shall in a period of 90 days from the day this Act comes into force appoint the members of the Council of the Agency.

(3) The Agency shall in a period of 60 days from the day of the application of this Act adopt its Statutes and submit them to the Croatian Parliament for confirmation.

(4) Until the Statutes of the Agency come into force, the Agency shall apply the provisions of the Statutes of the Croatian Securities Exchange Commission, except in any part that is in contravention to this Act.

(5) The Agency is bound, in a period of six months from the Statute's coming into force, to adopt the acts prescribed by this Act.

(6) Until the acts defined in the previous Paragraph are adapted, the Agency will settle issues that are important for its work by Decisions.

Article 25

On the day this Act will be applied, the following shall cease to be valid:

1) Provisions of Articles 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13 and 17 of the Securities Market Act (Official Gazette no 84/02);

2) The provisions of Articles 91, 92, 92a, 95, 96, 97, 98, 99, 100, 101, 102 and 103 of the Act on Compulsory and Voluntary pension Funds (Official Gazette no. 49/99, 63/00, 103/03 and 117/04);

3) The provisions of Articles 92 and 94 Paragraph 5 of the Act on Pension Insurance Companies and Payment of Pension Annuities on the Basis of Individual Capitalised Savings (Official Gazette, no 106/99 and 63/00);

4) The provisions of Articles 56, 57, 58, 59 and 60 of the Insurance Act (Official Gazette no. 9/94, 20/97, 46/97 revised wording, 116/99 and 11/02);

5) The provisions of Article 5 Paragraph 2, Article 7 Paragraph 3, Article 17 Paragraph 2, Article 21 Paragraph 2, Article 27 Paragraph 1 and Article 29 of the Insurance Brokerage and Representation Act (Official Gazette no. 27/99).

Article 26

(1) The period of office of the President and members of the Board of the Agency shall start on the day this Act will be applied.

(2) The periods of office and members of the Croatian Securities Exchange Commission, the director, deputy director, assistant directors and members of the Council of the Agency for Supervision of Pension Funds and Insurance and the directors and members of the Board of Management of the Directorate for Supervision of Insurance Companies shall cease on the day this Act will be applied.

Article 27

On the day this Act will be applied:

1) The Agency shall start working.

2) The Croatian Securities Exchange Commission, the Agency for Supervision of Pension Funds and Insurance and the Directorate for Supervision of Insurance Companies shall cease working.

3) All by-law regulations, except the Statutes as defined in Article 24 Paragraph 4 of this Act that govern the internal structure and organisation, the internal organisational form and the systematisation of jobs, the salaries and other material rights, the work and other rights of the Croatian Securities Exchange Commission, the Agency for Supervision of Pension Funds and Insurance and the Directorate for Supervision of Insurance Companies shall cease to be valid.

4) Employees of the Croatian Securities Exchange Commission, the Agency for Supervision of Pension Funds and Insurance and the Directorate for Supervision of Insurance Companies shall be taken on by the Agency with the application of the provision of Article 136 of the Labour Act (Official Gazette no. 137/04 revised wording) until the adoption of acts laying down the internal organisational form, employment conditions and work of employees of the Agency.

5) The Agency shall take into its possession the property and use of the office premises and equipment, all other real and moveable property and also all other rights of the Croatian Securities Exchange Commission, the Agency for Supervision of Pension Funds and Insurance and the Directorate for Supervision of Insurance Companies shall be transferred to it.

6) The Agency shall take over the monetary resources and accounts of the Croatian Securities Exchange Commission, the Agency for Supervision of Pension Funds and Insurance and the Directorate for Supervision of Insurance Companies.

8) The Agency shall become competent for all procedures and cases in the work of the scope of activities and competence of the Croatian Securities Exchange Commission, the Agency for Supervision of Pension Funds and Insurance and the Directorate for Supervision of Insurance Companies.

Article 28

This Act shall enter into force on the day of its publication in the Official Gazette of the Republic of Croatia and shall be applied from 1 January 2006.

ANNEX XVI Companies Act

ANNEX XVII Law on Associations

Membership

Article 4

(1) Any natural and legal person with capacity to act may, under the same conditions established by this Law and the statute of the association, become a member of an association.
(2) Persons with or without limited capacity to act may become members of an association without decision-making power in the association's bodies. The manner in which they may participate in the work of the association's bodies shall be prescribed by the statute of the association.
(3) An association shall keep a record of its members.

Foreign associations

Article 8

(1) A foreign association is, for the purpose of this Law, an association or other organizational form established without the intention of gaining profit, which fulfills the conditions prescribed by this Law, and which was established in accordance with the legal rules of the foreign state.
(2) A foreign association may conduct its activity in the Republic of Croatia after it is entered into the registry book of foreign associations by the ministry competent for the field of general state administration.
(3) In the Republic of Croatia a foreign association shall conduct its activity in accordance with this Law.

Statute of the association

Article 11

(1) An association shall have a statute.
(2) A statute is the basic general act of an association passed by the assembly. Other acts of an association, if there are any, must comply with the statute. An association may use a different name for a statute.
(3) The statute of an association shall contain the provisions regulating:
– name and the seat of the association,
– representation,
– aims,
– activities for the realization of aims,
– membership,
– bodies of the association, method of their election, their powers, their quorum and voting rule, and duration or their mandate,
– dissolution of the association
(4) The statute may contain the following provisions
– area of its activity,
– property and acquiring and use of property,
– modes of resolving disputes and conflicts of interest within the association,
– disciplinary responsibility of members,
– distribution of property after dissolution
– the logo of the association,
– other question of importance for the association.

Competent supervisory bodies

Article 26

(1) Members of the association shall supervise the activities of the association. If a member of the association notices shortcomings in the association's complying with its statute he/she may inform the authorized body of the associations, or in case that the statute does not envisage such body, the Assembly of the association. If the information is not considered by the statutory body or the Assembly within 30 days from the moment it was received and the shortcomings remained, the members have a right to file a suite with the competent county court in order to protect his/hers membership rights.
(2) Administrative supervision of the enforcement of this Law and regulations issued according to the Law shall be carried out by the ministry competent for general state administration.
(3) Inspectorate supervision shall be carried out by the county.

Procedure of inspectorate supervision

Article 27

(1) If state official empowered for inspectorate supervision over associations establishes that association has violated this Law or other laws, he may:
    1. order the elimination of detected shortcomings and irregularities in specified time- limit,
    2. instigate offence proceedings.
(2) State official of county office shall immediately inform the body of state administration in whose jurisdiction fall statutory goals of association of the taken measures in accordance with paragraph 1. If the official of the competent state administrative takes measures from the competence of that body, or if it starts offence procedure, he has a duty to immediately inform the county office

Offences

Article 39

(1) A fine of at least 1.000,00 but not exceeding 10.000,00 kunas shall be imposed on the association which:
    1. does not keep record of its members (Article 4 paragraph 3),
    2. performs activities that do not serve the realization of its statutory goals (Article 5 paragraph 1),
    3. does not use its name and abbreviated name in the form and content entered into registry book (Article 12 paragraphs 6 and 7),
    4. act in legal transactions in accordance with the changes and use the changed data before they have been entered into the register book of the associations (Article 19 paragraph 5).
(2) A fine between 500.00 and 5.000.00 shall be imposed on the legal representative for the offences from paragraph 1 of this Article.

ANNEX XVIII Act on Mutual Legal Assistance in Criminal Matters

Article 1

(1) This Act regulates mutual legal assistance in criminal matters (hereinafter: «mutual legal assistance»), unless provided otherwise by an international treaty.

(2) Mutual legal assistance is provided in respect of criminal acts the punishment of which, at the time of the request for assistance, falls within the jurisdiction of the judicial authorities of the requesting state.

(3) Mutual legal assistance may also be afforded in misdemeanour proceedings brought by the administrative authorities, in respect of acts which are punishable under the Croatian law by pecuniary fine, by virtue of being infringements of the rule of law and where in such proceedings the decision of the administrative authority may give rise to proceedings before a court having subject matter jurisdiction in criminal matters.

(4) Mutual legal assistance is also afforded in criminal proceedings referred to in paragraph 2 of this Article, and misdemeanour proceedings referred to in paragraph 3 of this Article, which are brought against legal persons.

(5) Mutual legal assistance is also afforded in respect of the European Court of Human Rights and the European Court of Justice, as well as in respect of other international and supranational organisations whose member the Republic of Croatia may become, if so stipulated in an international treaty.

Meaning of terms in this Act

Article 2

Terms and expressions used herein shall have the following meanings:

1. domestic competent authority – Ministry of Justice of the Republic of Croatia and/or domestic judicial authorities acting upon requests for mutual legal assistance,

2. domestic judicial authority – courts and state attorney's offices authorised by a special law to afford mutual legal assistance. In the context of this Act, a domestic judicial authority is also any administrative authority referred to in Article 1 paragraph 3 of this Act,

3. requesting state – a foreign state whose competent authority has transmitted the request for mutual legal assistance,

4. foreign competent authority – authority of the foreign state having jurisdiction, either pursuant to that county's law or pursuant to an international treaty, to transmit and receive requests for mutual legal assistance and/or the foreign judicial authority referred to in point 5 of this Article,

5. foreign judicial authority – foreign courts and other judicial authorities having jurisdiction, pursuant to the law of the foreign state, to act in criminal matters, including the foreign administrative authorities having jurisdiction in misdemeanour proceedings subject to conditions referred to in Article 1 paragraph 3 of this Act,

6. foreigner – a person of any other nationality other than Croatian,

7. extradited person – prosecuted or convicted person in the extradition proceedings, as of the moment of his placement under detention for the purpose of extradition.

Article 3

(1) In particular, this Act shall regulate the following:

1. mutual legal assistance in criminal proceedings pending in the Republic of Croatia or a foreign country (procuring and transmitting articles to be produced in evidence, service of writs and records of judicial verdicts, appearance before the court of witnesses for testimony and other acts necessary to carry out the court proceedings),

2. procedures of extradition to the Republic of Croatia of prosecuted or convicted persons based on verdicts of domestic courts,

3. acts of extradition of foreigners prosecuted or convicted based on judicial verdicts of the state requesting extradition,

4. acts of taking over and surrendering criminal prosecution,

5. acts of enforcement of foreign judicial verdicts in criminal matters.

(2) This Act shall not apply to arrests, the enforcement of verdicts or offences under military law which are not offences punishable under ordinary criminal law.

Article 4

Mutual legal assistance is afforded in the widest sense, in compliance with the principles of domestic legal order, principles of the European Convention for the Protection of Human Rights and Fundamental Freedoms and the International Covenant on Civil and Political Rights.

Article 5

A domestic competent authority shall decide on suitability and manner of execution of an act of mutual legal assistance from the request of a foreign judicial authority, unless provided otherwise by the provisions of this Act or an international treaty.

Authorities competent to afford mutual legal assistance and the channels of communication

Article 6

(1) Domestic judicial authorities transmit the requests for mutual assistance and information referred to in Article 18 paragraph 1 of this Act to foreign competent authorities through the Ministry of Justice.

(2) The Ministry of Justice has jurisdiction to receive requests for mutual assistance of foreign competent authorities, and transmit them without delay to domestic judicial authorities, unless evident that the request should be refused.

(3) The Ministry of Justice may return the request to the foreign competent authority for corrections or supplements and determine an appropriate deadline for delivery of so corrected, i.e. supplemented request. After the expiry of the deadline, the request shall be executed according to the status in the judicial record.

(4) As an exception to paragraph 1 of this Article, domestic judicial authorities may directly address the request for mutual legal assistance to a foreign judicial authority, when so explicitly provided by the provisions of this Act and subject to condition of reciprocity, or when such a communication is envisaged by an international treaty (direct communication).

(5) In cases of direct communication referred to in paragraphs 4 and 7 of this Article, a domestic judicial authority shall communicate a copy of the request for mutual legal assistance to the Ministry of Justice.

(6) In urgent cases and subject to reciprocity, the Ministry of Justice may transmit and receive requests for mutual legal assistance through the Interpol.

(7) In cases of direct communication referred to in paragraph 4 of this Article, domestic judicial authorities may, provided they fulfill the obligation referred to in paragraph 5 of this Article, transmit and receive requests for mutual legal assistance through the Interpol.

(8) The Ministry of Justice shall transmit and receive through the Ministry of Foreign Affairs the requests for mutual legal assistance to/from a foreign state that has no international treaty in force with the Republic of Croatia, as well as in cases when an international treaty envisages use of special diplomatic channels.

Form and mandatory contents of the request

Article 8

(1) Domestic judicial authority shall act upon the request for mutual legal assistance of a foreign judicial authority if the request was transmitted in writing. The request, as well as attached documents, have to be accompanied by the translation into Croatian, and if this is not possible, into English. The translations have to be officially certified.

(2) A domestic judicial authority shall act upon a request for mutual legal assistance of a foreign judicial authority even if the request was transmitted via electronic or some other telecommunications means which provide written record, if it may establish its authenticity and if the foreign competent authority is willing, upon request, to deliver a written evidence on the manner of transmission and the original request.

(3) Unless provided otherwise by an international treaty or the provisions of this Act, the request for mutual legal assistance shall indicate the following:

1. place of issuance and the name of the competent authority making the request,

2. legal grounds to afford mutual legal assistance,

3. detailed description of an act of mutual legal assistance sought and the reason for the request,

4. legal title, short factual and legal description of the criminal offence (unless the request refers to service of judicial
verdicts, depositions of parties, documents and alike),

5. exact data and nationality of the person concerned and his status in the proceedings,

6. in case of service of judicial writs, also the type of the writ to be served.

Particularities in the manner of executing the request

Article 10

(1) When affording mutual legal assistance, domestic judicial authority shall comply with the formalities and procedures expressly indicated in the request as necessary pursuant to the law of the

requesting state, unless provided otherwise by an international treaty and provided that such formalities and procedures are not contrary to the principles of the domestic legal order.

(2) Domestic judicial authority executes the request of a foreign judicial authority without delay, taking into account procedural deadlines, as well as other specially determined deadlines explained in the request.

(3) If a domestic judicial authority may foresee that it shall not be able to observe a specially determined deadline for execution of the request, while the explanation referred to in paragraph 2 of this Article expressly indicates that each postponement will lead to significant disruption of procedure before a foreign judicial authority, the domestic judicial authority shall indicate without delay the required time to execute the request. Domestic and foreign judicial authorities may thereafter agree on further acts required to be undertaken in connection with the request.

(4) If the request of a foreign judicial authority may not be executed, or may not be executed fully in compliance with the required conditions, the domestic judicial authority shall without delay inform the foreign judicial authority to this effect, indicating the conditions under which such request may be executed.

Refusal of the request

Article 12

(1) Domestic competent authority may refuse the request for mutual legal assistance:

1. if the request concerns an offence which is considered to be a political offence, an offence connected with a political
offence,

2. if the request concerns a fiscal offence,

3. if the execution of the request would prejudice the sovereignty, security, legal order or other essential interests of the Republic of Croatia,

4. if it may reasonably be assumed that a person whose extradition is claimed would be in case of extradition criminally prosecuted or punished on account of his race, religious beliefs, nationality, affiliation with a particular social group or on account of his political beliefs, i.e. that that person's position may be prejudiced for any of these reasons,

5. if it concerns an insignificant criminal offence.

(2) Criminal offences or attempts to commit criminal offences against the values protected by international law, and participation in execution of such criminal offences, may not serve as basis for refusal of the request for mutual legal assistance in the context of paragraph 1 point 1 of this Article.

(3) Request for mutual legal assistance concerning the fiscal offence referred to in paragraph 1 point 2 of this Article shall not be refused solely based on the grounds it concerns an offence which is considered to be a fiscal offence pursuant to domestic law.

Special cases of communicating information on criminal offences

Article 20

(1) When the request for mutual legal assistance concerns a criminal offence related to trafficking in humans and slavery, money laundering, counterfeiting money, illicit production, processing and sale

of narcotic substances and poisons, production and dissemination of pornographic material, criminal offences related to organized crime and terrorism, and other criminal offences for which centralisation of data has been provided under international agreements, the domestic judicial authority conducting criminal proceedings, i.e. authority affording mutual legal assistance, shall be bound immediately to transmit the data on such criminal offences and perpetrators to the Ministry of Interior, while the first-instance court shall in addition transmit a final verdict.

(2) If the request for legal assistance concerning the criminal offences referred to in paragraph 1 of this Article was forwarded to or received directly within the context of Article 8 paragraph 2 of this Act, the domestic judicial authority shall also transmit without delay the data referred to in paragraph 1 of this Article to the Ministry of Justice.

(3) At least once a year, the Ministry of Justice shall notify the foreign competent authority of all criminal convictions and measures in respect of nationals of that foreign state, entered into judicial records, unless provided otherwise by an international treaty.

(4) Upon a request of a foreign competent authority, the Ministry of Justice shall transmit in each individual case a transcript of the verdicts and measures on which it delivered notification, in the context of paragraph 3 of this Article, and it may also deliver other information that it deems might be useful for subsequent measures at the requesting state.

Taking over the proceedings by the Republic of Croatia

Article 62

Upon request of a foreign judicial authority, the domestic judicial authority may take over carrying out criminal proceedings for a criminal offence committed abroad:

1. when extradition is not allowed,

2. if a foreign judicial authority stated that if shall not further criminally prosecute the prosecuted person after the final decision of the domestic judicial authority.

Surrender of the criminal proceedings

Article 65

(1) If a foreigner domiciled in a foreign county committed an offence in the territory of the Republic of Croatia, criminal prosecution may be surrendered to that country, provided it does not object thereto.

(2) Criminal prosecution may be surrendered for offences with prescribed punishment up to ten years of imprisonment.

ANNEX XIX Leasing Act - Extract

Data confidentiality requirement

Article 86

(1) Members of different bodies of the leasing company, shareholders, stakeholders in the leasing company, employees of the leasing company and other persons who have access to the data referred to in Article 85 of this Act, through their affiliation with the leasing company or via rendering services to the leasing company, shall not disclose such data to third parties, shall not use them against the leasing company or its clients and shall not enable third parties to use such data.

(2) The data confidentiality requirement shall not apply in the following cases:

1. The concerned part explicitly, in writing, agrees on release of certain confidential data;
2. The competent court requests, in writing, or orders submission of such data for determining facts in offence procedures;
3. In cases of individual regulations on money laundering prevention;
4. The data is required for legal decisions, in litigation procedures, on the relation between the lessor and the lessee, and/or the vendor, and/or other parties entitled to certain rights on the basis of the lease agreement;
5. The competent court requests, in writing, or orders submission of such data in relation to probate procedures;
6. The competent court requests, in writing, or orders submission of such data for the purposes of execution of claims against the property of the lessee or other party entitled to rights based on the lease agreement;
7. For the purposes of supervision activities conducted by the Agency and/or other supervisory body;
8. Disclosing to the Agency for the purposes of maintaining the Register of Leased Assets;
9. Disclosing to the tax authority, for the needs of its mandated operations.

(3) Data confidentiality requirements shall apply to the parties referred to in paragraph 1 of this Article even after termination of their employment in the leasing company and/or after termination of their status as shareholders, stakeholders or members in the bodies of the leasing companies.

(4) The supervisory body and/or other institutions and courts may use the data they received pursuant to paragraph 2 of this Article only for the intended purpose.

ANNEX XX Bilateral and Multilateral International Treaties (Conventions)

Bilateral and Multilateral International Treaties (Conventions) in the field of the international legal assistance and cooperation concerning civil and criminal matters and extradition

1. Albania- Convention on the Issuing of Culprits, 22. June 1926.
2. Memorandum of Conformity on Cooperation between the State Attorney of the Republic of Croatia and Public Attorney of the Republic of Albania Concerning Transnational Crime and Money Laundry acquired by the crime
3. Algeria - Treaty on Mutual Assistance Concerning Legal Actions in Civil and Criminal Matters from 31. March 1982.
4. Treaty with Australia on the Mutual Extradition of Culprits, Belgrade, 6. December 1900.
5. Treaty with Australia on the Exchange of the Official Publications, Cambera, 19. November 1953.
6. Treaty on the Mutual Legal Traffic between FNRJ and the Republic of Austria, Vienna, 16. December 1954.
7. Treaty with Austria on The Mutual Acknowledgement and the Implementation of the Decisions on Sustenance, Vienna, 10. October 1961.
8. Treaty with Austria on Extradition, Belgrade, 1. February 1982.
9. Treaty with Austria on the Mutual Implementation of the Court Decisions Concerning Criminal Matters, Belgrade, 1. February 1982.
10. Treaty with Austria on Legal Assistance Concerning Criminal Matters, Belgrade, 1. February 1982.
11. Treaty with Austria on the Mutual Acknowledgement and Implementation of the Decisions of the Chosen Courts and the Settlements Concerning Commercial Matters reached in front of the Chosen Courts, Belgrade, 18. March 1960.
    a. Treaty between the Republic of Croatia and the Republic of Austria on the Annex of the European Convention on the Mutual Legal Assistance Concerning Criminal Matters, in the text with the additional Protocol to the European Convention on the Mutual Legal Assistance Concerning Criminal Matters and the Facilitation of its Application.
12. Memoranda of understanding between Ministry of Justice of the Republic of Croatia and Federal Ministry of Justice of the Republic of Austria
13. The Convention on Extradition and the Legal Assistance Concerning Criminal Matters between the former Yugoslavia (SFRJ) and the Kingdom of Belgium, Beograd, 4. June 1971.
14. Treaty between the Governments of the Republic of Croatia, Bosnia and Herzegovina and the Federation of Bosnia and Herzegovina on the Legal Assistance Concerning Civil and Criminal Matters, Split, 26. February 1996. (the application area- the Federation of Bosnia and Herzegovina).
    a. Treaty between the Republic of Croatia and Bosnia and Herzegovina on the Amendments of the Treaty between the Government of the Republic of Croatia, the Government of Bosnia and Herzegovina and the Government of the Federation of Bosnia and Herzegovina on the Legal Assistance Concerning Civil and Criminal Matters, signed on 17. 06. 02.
15. Treaty between the Governments of the Republic of Croatia, Bosnia and Herzegovina and the Federation of Bosnia and Herzegovina on the Mutual Implementation of the Court Decisions Concerning Criminal Matters, 26. February 1996.
16. Treaty between the Republic of Croatia and Bosnia and Herzegovina on the Amendments of the Treaty between the Governments of the Republic of Croatia, Bosnia and Herzegovina and the Federation of Bosnia and Herzegovina on the Legal Assistance Concerning Criminal Matters, signed on 07. 06. 04.
17. Agreement between the Republic of Croatia and Bosnia and Herzegovina on the amendments of the Agreement on Mutual Implementation of the Court Decisions Concerning Criminal Matters

18. Treaty between the Federative National Republic of Yugoslavia and the National Republic of Bulgaria, Sophia, 23. March 1956.
19. Treaty between the Former Yugoslavia (SFRJ) and Republic of Cyprus on Mutual Assistance Concerning Legal Assistance in Civil and Criminal Matters from 19. September 1984.
20. Treaty between the Republic of Croatia and the Republic of Montenegro on extradition
21. Treaty on the Regulation of Legal Relations Concerning Civil, Family and Criminal Matters between the Former Yugoslavia(SFRJ) and Czech Republic, Belgrade, 20. January 1964.
22. Treaty between the former Yugoslavia (SFRJ) and the former Czech Republic(ČSSR) on the Mutual Convicts Extradition for the purpose of Serving a Term, Prague, 23. May 1989.
23. Treaty between the former Yugoslavia (SFRJ) and the Kingdom of Denmark on the Mutual Convicts Extradition for the purpose of Serving a Term, Belgrade, 28. October 1988.
24. Convention on the Mutual Legal Assistance Concerning Criminal Matters between the former Yugoslavia(SFRJ) and the Republic of France, Belgrade, 29. October 1969.
25. Convention on the Issuing of Persons between the former Yugoslavia (SFRJ) and the Republic of France, Paris, 23. September 1970.
26. Convention between FNRJ and the Kingdom of Greece on the Mutual Legal Relations, Athens, 18. June 1959.
27. Agreement between FNRJ i the Kingdom of Greece on the Mutual Acknowledgement and the Implementation of the Court Acts – Decisions, Athens, 18. June 1959.
28. Italy - Convention on the Issuing of Culprits since 6. April 1922.
29. Italy - Convention on the Legal and Court Protection of the respective citizens since 6. April 1922.
30. Treaty between the former Yugoslavia (SFRJ) and the NR of Hungary on the Mutual Legal Traffic since 7. March 1968.
31. Treaty on the Amendments of the Treaty on the Mutual Legal Traffic, Belgrade, 7. March 1968, ratified on 25. April 1986.
32. Treaty between the Republic of Croatia and the Republic of Macedonia on the Legal Assistance Concerning Civil and Criminal Matters, signed in Skopje on 2. September 1994.
33. Treaty between the Republic of Croatia and the Republic of Macedonia on the Mutual Implementation of the Court Decisions Concerning Criminal Matters, signed in Skopje on 2. September 1994.
34. Treaty on Legal Assistance in Civil, Family and Criminal Matters from 8th of June 1981
35. Treaty on the Issuing of Culprits since 28.02. (11.03) 1896.
36. Agreement on the Mutual Culprits Extradition since 6. December 1900.
37. The exchange of Notes Concerning the Amendments of the Treaty on the Mutual Culprits Extradition since 6. December 1900., in relation to specific mandated territories since 7. December 1927., 27. August 1928. and since 22.October 1928.
38. Germany-Treaty on the Legal Assistance Concerning Criminal Matters since 1. October 1971.
39. Germany- Agreement on Extradition since 26. November 1970.
40. Treaty between the Government of FNRJ and the Government of the NR of Poland on the Legal Actions Concerning Civil and Criminal Matters, ratified in Warsaw on 6. February 1960.
41. Romania- Treaty on the Legal Assistance since 18. October 1960.
42. Romania- The additional Protocol Concerning the Treaty on the Legal Assistance since 18. October 1960., ratified on 21. January 1972.
43. Treaty between FNRJ and U.S.S.R. on the Legal Assistance Concerning Civil, Family and Criminal Matters, Moscow, 24. February 1962.
44. United States of America - The Convention on the Issuing of Culprits since 12/25. October 1901.

45. Treaty between the Republic of Croatia and the Republic of Slovenia on the Legal Assistance Concerning Civil and Criminal Matters, Zagreb, 7. February 1994.
46. Treaty between the Republic of Croatia and the Republic of Slovenia on the Mutual Implementation of the Court Decisions Concerning Criminal Matters, Zagreb, 7. February 1994.
47. Treaty between the Republic of Croatia and the Republic of Slovenia on Extradition, Brdo near Kranj, 8. July 1994.
48. Slovakia- Treaty on the Regulation of the Legal Relations Concerning Civil, Family and Criminal Matters between the former Yugoslavia(SFRJ) and the ČSSR, Belgrade, 20. January 1964.
49. Slovakia- Treaty between SFRJ and the ČSSR on the Mutual Convicts Extradition for the purpose of Serving a Term, Prague, 23. May 1989.
50. Treaty between the Republic of Croatia and the Former Republic of Yugoslavia on the Legal Assistance Concerning Civil and Criminal Matters, signed in Belgrade, on 15. September 1997.
51. Treaty on Extradition between the Republic of Croatia and the Republic of Serbia
52. Agreement between the Government of the former Yugoslavia(SFRJ) and the Government of the Kingdom of Spain on the Legal Assistance Concerning Criminal Matters and the Issuing of Culprits, Belgrade, 8. July 1980.
53. Convention with the Swiss Confederation on the Issuing of Culprits, Vienna, 28. November 1887.
54. Convention between the former Yugoslavia(SFRJ) and the Republic of Turkey on the Legal Assistance Concerning Criminal Matters, Ancara, 8. October 1973.
55. Convention on Issuing between the former Yugoslavia(SFRJ) and the Republic of Turkey since 17. November 1973.
56. The United Kingdom Of Great Britain And Northern Ireland- Treaty on the Mutual Culprits Extradition between the Kingdom of Serbia and Great Britain, Belgrade, 6. December 1900.
57. The United Kingdom Of Great Britain And Northern Ireland- The exchange of the Notes on the Amendments of the Treaty on the Mutual Culprits Extradition since 6. December 1900., in relation to specific mandated territories since 7. December 1927., 27. August 1928., and 22. October 1928.

Multilateral International Treaties Concerning International Legal Assistance and Cooperation in Criminal and Civil Matters

Council of Europe Instruments on Mutual Legal Assistance in Criminal Matters:

1. European convention on mutual legal assistance in criminal matters, of 20 April 1959
2. Additional protocol to the European convention on mutual legal assistance in criminal matters, of 17 march 1978
3. Second additional protocol to the European convention on mutual assistance in criminal matters, of 8 November 2001

Council of Europe Instruments on Extradition and Criminal Matters in General:

4. European convention on extradition, of 13 December 1957
5. Additional protocol to the European convention on extradition, of 15 October 1975
6. Second additional protocol to the European convention on extradition, of 17 march 1978
7. Convention on the transfer of sentenced persons, of 21march1983
8. Convention on laundering, search, seizure and confiscation of the proceeds from crime, 8 November 1990
9. Convention on cybercrime of 23 November 2001
10. Additional protocol to the convention on cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems

11. European convention on the compensation of victims of violent crimes

Council of Europe Convention on Action against Trafficking in Human Beings, of 16 May 2005

United Nations Instruments in Criminal Matters-Organized Crime:

12. UN convention against transnational organized crime, of 15 November 2000
13. Protocol to prevent, suppress and punish trafficking in persons, especially women and children, supplementing the un convention against transnational organized crime, of 15 November 2000
14. Protocol against the smuggling of migrants by land, sea and air, supplementing the un convention against transnational organized crime, of 15 November 2000
15. Protocol against illicit manufacturing of and trafficking in firearms, their parts and components and ammunition, supplementing the un convention against transnational organized crime, of 31/05/2001
16. UN convention against illicit traffic of narcotic drugs and psychotropic substances, of 20 December 1988

Council of Europe Instruments in Criminal Matters – Corruption:

17. Civil law convention on corruption, of 4 November 1999
18. Criminal law convention on corruption of 27 January 1999
19. Additional protocol to the criminal law convention on corruption, of 15 may 2003

United Nations Instruments in Criminal Matters- Corruption

20. United nations convention against corruption, of 31 October 2003

Council of Europe Instruments in Criminal Matters –Terrorism

21. European convention on the suppression of terrorism, of 27 january1977
22. Protocol amending the European convention on the suppression of terrorism, of 15 may 2003

Council of Europe Convention on the Prevention of Terrorism, of 16 May 2005

United Nations Instruments in Criminal Matters-Terrorism

23. Convention on offences and certain other acts committed on board aircraft, of 14 September 1963
24. Convention for the suppression of unlawful seizure of aircraft, of 16 December 1970
25. Convention for the suppression of unlawful acts against the safety of civil aviation , of 23 September 1971
26. Protocol on the suppression of unlawful acts of violence
27. At airports serving international civil aviation, supplementary to the convention for the suppression of unlawful acts against the safety of civil aviation, of 23 September 1971
28. Convention on the prevention and punishment of crimes against internationally protected persons, including diplomatic agents , of 14 December 1973
29. Convention on the physical protection of nuclear material, of 26 October 1979
30. International convention for the suppression of the financing of terrorism, of 9 December 1999
31. International convention against taking of hostages, of 17 December 1979
32. Convention on the marking of plastic explosives for the purpose of detection, of 01 march 1991
33. International convention for the suppression of terrorist bombings, of 15 December 1997

34. Convention for the suppression of unlawful acts against the safety of maritime navigation, of 10 march 1988
35. Protocol for the suppression of unlawful acts against the safety of fixed platforms located on the continental shelf , of 10 march 1988
36. International convention for the suppression of acts of nuclear terrorism

<u>On cooperation in combating organised crime, international terrorism and other especially dangerous crimes</u>

1. Treaty on cooperation between the Government of the Republic of Croatia and the Government of the Republic of Albania in the fight against terrorism, smuggling and drug abuse, and against organised crime (Zagreb, 14/12/1993);
2. Agreement between the Government of the Republic of Croatia and the Government of the Republic of Bulgaria on Police Cooperation (Sofia, 27/5/2011);
3. Treaty between the Government of the Republic of Croatia and the Government of the Czech Republic on cooperation in the battle against organized crime, illegal trafficking of narcotics and psychedelic substances, terrorism and other forms of dangerous criminal activities (Prague, 30/11/1999);
4. Agreement between the Government of the Republic of Croatia and the Government of the Arab Republic of Egypt on Cooperation in the Field of Crime Combats (Kairo, 22/11/2004);
5. Cooperation Agreement between the Government of the Republic of Croatia and the Government of the Republic of India on combating international illicit trafficking in narcotic drugs and psychotropic substances, international terrorism and organized crime (New Delhi, 4/5/2001);
6. Treaty between the Government of the Republic of Croatia and the Government of the Republic of Italy on the battle against the international illegal trade of narcotics and psychedelic substances, and organized crime (Rome, 28/5/1993);
7. Agreement between the Government of the Republic of Croatia and the Government of the Republic of Latvia on co-operation in combating terrorism, illicit drug trafficking and organized crime (Zagreb, 23/2/2001);
8. Treaty on the cooperation between the Government of the Republic of Croatia and the Government of the Republic of Macedonia in the battle against the international illegal trade of illicit drugs and psychedelic substances, international terrorism and organized crime (Zagreb, 12/4/1996);
9. Agreement between the Government of the Republic of Croatia and the Government of Romania on the cooperation in the combating terrorism, organized crime, illicit trafficking in drugs and psychotropic substances and other illegal activities (Zagreb, 30/9/2000);
10. Treaty between the Government of the Republic of Croatia and the Government of the Republic of Slovenia on cooperation in the battle against terrorism, smuggling and drug abuse as well as against organized crime (Zagreb, 4/6/1993);
11. Agreement between the Government of the Republic of Croatia and the Government of the Kingdom of Sweden regarding cooperation in combating crime (Zagreb, 3/10/2005);
12. Memorandum of understanding on cooperation in the fight against serious crime, organized crime, illict drug trafficking, people smuggling, human trafficking, international terrorism and in like matters of mutual interests between the Ministry of Interior, the Ministry of Finance and the Public Attorney's Office of the Republic of Croatia and the Association of Chief Police Officers, the Crown Prosecution Service of England and Wales, the Serious Fraud Service, Her Majesty's Customs and Excise, the United Immigration Service, the National Crime Squad and the National Criminal Intelligence Service of the United Kingdom of Great Britain and Northern Ireland (Zagreb, 1/3/2002);
13. Agreement between the Government of the Republic of Croatia and the Council of Ministers of Bosnia and Herzegovina on Cooperation in State Border Control (Sarajevo, 29/3/2007);
14. Agreement between the Republic of Croatia and the Republic of Austria on Police Co-operation (Vienna, 14/11/2007);

15. Agreement between the Government of the Republic of Croatia and the Government of the Republic of Hungary on Cooperation in the Fight Against Cross-border Crime (Hèviz, 3/10/2008);
16. Agreement between the Government of the Republic of Croatia and the Government of the French Republic on Police Co-operation (Paris, 10/10/2007);
17. Agreement between the Government of the Republic of Croatia and the Government of the Hellenic Republic on fighting against international illicit trafficking of narcotics drugs and psychotropic substances, international terrorism and organized crime (Athens, 23/11/1998);
18. Agreement between the Government of the Republic of Croatia and the Government of the State of Israel on Cooperation in the Fight Against Crime (Jerusalem, 16/9/2009);
19. Agreement between the Government of the Republic of Croatia and the Government of the Republic of Serbia on Police Cooperation (Rijeka, 25/9/2009);
20. Agreement between the Government of the Republic of Croatia and the Government of the Republic of Moldova on cooperation in combating organized crime, illicit trafficking in narcotic drugs and psychotropic substances, terrorism as well as other kinds of serious crime (Kishinev, 16/2/2006);
21. Agreement between the Government of the Republic of Croatia and the Government of Malta on the Fight against Illicit Trafficking in Narcotic Drugs and Psychotropic Substances, Organized Crime and International Terrorism (Zagreb, 7/4/2010);
22. Agreement between the Government of the Republic of Croatia and the Government of the Slovak Republic on Police Cooperation (Zagreb, 17/11/2010);
23. Agreement between the Government of the Republic of Croatia and the Government of the United States of America On Enhancing Cooperation in Preventing and Combating Serious Crime (Washington, 16/2/2011);
24. Agreement between the Government of the Republic of Croatia and the Bosnia and Herzegovina Council of Ministers on Fighting Cross-Border Crime (Sarajevo, 17/9/2010);
25. Agreement between the Government of the Republic of Croatia and the Government of the Republic of Slovenia on cross-border police cooperation (Zagreb, 6/11/2002);
26. Agreement between the Government of the Republic of Croatia and the Government of the Federal Republic of Germany on Cooperation in Fighting Organized Serious Crime (Berlin, 10/3/2009);
27. Agreement Between the Government of the Republic of Croatia and the Government of the Republic of Kazakhstan on the Cooperation in Combating Organized Crime, Illicit Trafficking in Narcotic Drugs and Psychotropic Substances, Terrorism and Other Types of Crime (Astana, 5/7/2007);
28. Agreement on Cooperation between the Government of the Republic of Croatia and the Government of the Republic of Chile on the Prevention and Control of Abuse and Illicit Trafic in Narcotic Drugs and Psychotropic Substance (Santiago, 15/6/2001);
29. Treaty on cooperation between the Government of the Republic of Croatia and the Government of Ukraine in the battle against terrorism, smuggling and drug abuse, and against organized crime (Kiev, 26/10/1993);
30. Cooperation agreement between the Government of the Republic of Croatia and the Government of the Republic of Turkey on fighting against international illicit trafficking in narcotic drugs and psychotropic substances, international terrorism and organized crime (Ankara, 7/11/1995);
31. Agreement between the Government of the Republic of Croatia and the Government of the Democratic Socialist Republic of Sri Lanka on cooperation in combating international illict trafficking in narcotic drugs and psychotropic substances, international terrorism and organized crime (Colombo, 7/5/2001);
32. Convention between the Government of the Republic of Croatia and the Government of the Kingdom of Belgium on Police Co-operation (Zagreb, 19/10/2004);
33. Agreement between the Government of the Republic of Croatia and the Government of the Republic of Poland on cooperation in the fight against crime (Dubrovnik, 9/7/2010);

34. Agreement between the Government of the Republic of Croatia and the Government of Montenegro on Police Cooperation (Budva, 17/3/2011);
35. Agreement between the Government of the Republic of Croatia and the Government of the Italian Republic on Cross-border Police Cooperation (Zagreb, 5/7/2011);
36. Agreement between the Republic of Croatia and the Kingdom of Spain on Fight Against Crime and on Security Issues (Madrid, 24/10/2011);
37. Agreement between the Government of the Republic of Croatia and the Government of the Republic of Macedonia on police cooperation (Skopje, 28/5/2012).

ANNEX XXI Confiscation of Pecuniary Gain Acquired by a Criminal Offence in 2011

County and municipal state attorneys' offices

Criminal Offence	No. of security measures	Amount secured through freezing	No. court rulings	Amounts
Art. 173.st.2 CC			67	162,225
Art. 177. CC			1	3
Art. 195. CC			26	114,270
Art. 216.1 CC	9	1,331	201	70,229
Art. 217/1 CC	3	5,256	357	314,354
Art. 218. CC		0	62	62,032
Art.219. CC		0	3	460
Art. 220. CC	1	55,141	8	192,913
Art. 224. CC	7	756,498	103	1,141,942
Art. 224.a CC		0	10	10,271
Art. 226		0	2	4,036
Art. 227. CC		0	2	20,204
Art. 330. CC		0	1	65
Art. 234. CC		0	7	21,238
Art. 235. CC		0	2	5
Art. 236. CC		0	5	731
Art. 259. CC		0	1	55
Art. 261. CC	1	6,749,001		0
Art. 274. CC		0	1	0
Art. 282 CC	1	3,702,991		0
Art. 286. CC		0	4	594,249
Art. 287. CC		0	1	4
Art. 292. CC	2	6,829,877	25	2,428,341
Art. 293 CC	1	260,000	13	431,373
Art. 297. CC		0	1	2
Art. 298 CC		0	5	0
Art. 311. CC		0	2	241
Art. 317. CC		0	1	104
Art. 330. CC		0	1	65
Art. 337. CC	42	8,705,381	32	2,186,354
Art. 344. CC	1	83,522		0
Art. 345. CC		0	19	135,186
Art. 33 Law on Energy		0	2	1,979
Total	68	27,148,999	965	7,902,082

USKOK

Criminal Offence	No. of security measures	Amount secured through freezing	No. court rulings	Amounts
Art. 294.a CC	1	731,278		0
Art.,177/3,CC		0	7	205,690
Art.,173/3,CC	1	122	10	1,545,948
Art.,218/2,CC,		0	1	41,095
Art.,298/1,CC,		0	5	100,230
Art.,333/3,i,217/2, CC,	1	89,817	3	28,876
Art.337.,CC,	8	2,922,265	7	40,002
Art.,343/1,CC,	1	0	3	155,596
Art.,347.,CC	2	2,210,000	14	149,851
Art.,348.,CC,		0	5	112,553
Total	14	6,075,560	55	2,379,842

Grand,total

USKOK and State Attorney's Office	No. of security Measures	Amount secured through freezing	No. court rulings	Amounts
Grand total	82	33,224,559	1,020	10,281,924

ANNEX XXII Civil Servants Act

Chapter II

Duties of Civil Servants

Section 1

Conduct of Civil Servants

Article 15

Performance of Duties and Obligation to Adhere to Laws

(1) Civil servants shall be obliged to perform their duties as foreseen in their post description correctly, duly, conscientiously and professionally, not exploiting them for personal gain, in compliance with the principle of public accessibility, adhering to the constitutional and legal order of the Republic of Croatia.

Article 16

Abuse of Authority

(1) In performance of their duties, civil servants shall be obliged to act in compliance with the principles of legality and protection of the public interest, and they are prohibited from abusing their authority to achieve personal interests or the interests of some other natural or legal person.

Article 17

Refusal of Proffered Gifts

(1) Civil servants shall be prohibited from seeking or receiving gifts for their personal gain, or for the gain of their family or an organisation, or for favourable settlement of an administrative or other proceeding.

Article 18

Unwarranted Rewarding of Other Civil Servants

(1) Civil servants may neither offer nor give gifts or other benefits to other civil servants, their relatives or spouses or common-law partners for personal gain.

Article 19

Providing Information and Explanations on Administrative Affairs

(1) Civil servants shall be obliged to provide the public with the necessary information on performed tasks pursuant to regulations governing access to information.

(2) Civil servants shall be obliged to secure explanations for all procedures conducted and decisions made during performance of their duties.

Article 20

Timely and Cost Efficient Performance of Duties

(1) Civil servants shall be obliged to perform their duties in a cost effective and timely manner, and pursuant to law they shall render legal assistance, avoiding unjustifiably complex or scarcely foreseeable procedures and preventing situations that may lead to conduct damaging to preservation of the legal interests of the State or their clients.

Article 21

Non-disclosure of Official Secrets and Respect for Privacy

(1) Civil servants shall be obliged to maintain as secrets all data to which they gain knowledge during procedures concerning clients and their rights and obligations and legal interests pursuant to law.

(2) Civil servants shall be obliged to maintain official or other secrets as specified by law or other regulations. The obligation to maintain official or other secrets shall continue for a period of five years after departure from the civil service, unless specified otherwise by separate legislation.

(3) The chief executive of a State body may exempt civil servants from the obligation to maintain official or other secrets in judicial or administrative proceedings if this involves data essential to ascertain the facts and decision-making in a given case.

Article 22

Professional Conduct

(1) Civil servants shall be obliged to ensure a high quality of professionalism in their work, improving their professional skills and participating in additional professional training for personal advancement and enhancement of the efficiency of the civil service.

(2) The State body shall be responsible for the ongoing professional refinement of civil servants through organisation of workshops, exercises, seminars, courses, etc.

Article 23

Presence at the Workplace

(1) Civil servants shall be obliged to observe the designated work hours of the body in which they are employed and use such time to perform their duties, and they shall be present at their workplace pursuant to the conditions of the service.

(2) During work hours, civil servants may not leave the workplace without approval from the superior civil servant, except for use of daily rest breaks, while in cases of emergencies they must excuse their absence immediately upon returning.

(3) Civil servants shall be obliged to notify their immediate superiors of inability to come to the workplace, and of the reasons therefore within a period of 24 hours after their emergence, unless unable to do so due to objective reasons or force majeure, in which case they shall be obliged to notify their immediate superiors immediately after the reasons for their inability to effect notification cease. Civil servants shall not be entitled to salaries for the duration of their unexcused absence from work.

(4) The Government shall issue a directive to regulate the possibility of work at separate sites ("remote work") and part-time work.

Article 24

Use of Property

(1) Civil servants shall be obliged to use the property entrusted to them for the purposes of performing their duties with due care and they may not use said property for personal gain or other, illegal activity.

Article 25

Personal Conduct

(1) Civil servants shall behave in a manner that neither diminishes their own reputation nor the reputation of the civil service, and does not compromise their impartiality in performance of their duties. (2) The codes of conduct for civil servants shall be governed by the code of ethics of the Government of the Republic of Croatia.

TERMINATION OF CIVIL SERVICE

Article 132

Termination of Civil Service

(1) Civil service shall be terminated:

a) by agreement,
b) expiry of a deadline,
c) dismissal,
d) by force of law, and
e) in another manner specified by law.

or whose civil service ends by force of law.

Article 133

Resolutions on Termination of Civil Service

(1) A resolution shall be issued on termination of civil service.

(2) The resolution specified in paragraph (1) shall be issued within a period of eight days after circumstances arise which are the cause for termination of service.

Article 134

Termination of Fixed-term Civil Service

(1) Fixed-term civil service shall cease upon expiry of the specified period, provided that it does not cease earlier in some other legally-stipulated manner.

Article 135

Consensual Termination of Civil Service

(1) Civil service may be terminated pursuant to a written agreement between the civil servant and the chief executive of the State body whereby the date of termination is determined.

Article 136

Dismissal from Civil Service

(1) A civil servant shall be dismissed from the civil service if he/she does not perform satisfactorily in trial work, and service shall formally cease as of the date on which the resolution on termination of service becomes final.

(2) Civil service may be terminated on the basis of a written resignation tendered to the State body by the civil servant.

Article 137

Termination of Civil Service by Force of Law

(1) Civil service for a civil servant shall terminate by force of law:

a) in case of death,
b) by establishment of right to pension due to general inability to work – on the date of legal entry into force of the relevant resolution,
c) when he/she reaches the age of 65 and has not less than 20 years of work service for pension eligibility – as of the last day in the year in which such conditions arise,
d) when he/she is unconditionally sentenced to imprisonment for a period exceeding six months – as at the date on which the conviction becomes final,
e) when he/she is convicted for a crime as specified in Article 45 hereof – as at the date on which the conviction becomes final,
f) when he/she is absent from work for five consecutive days without excuse – as of the date of departure from the service or the first day of absence from work,
g) if he/she does not take the civil service examination within the stipulated period – upon expiry of the deadline within which he/she was obliged to take the civil service examination,
h) if it is ascertained that upon admission to the civil service he/she did not meet admission criteria as specified herein – as of the date of such ascertainment,
i) when it is ascertained that at the time of admission to the civil service there were bars to such admission as stipulated herein – as of the date of such ascertainment,

j) when the sanction of dismissal from the civil service is imposed due to severe breaches of official duties – as of the date on which the decision of the civil service tribunal becomes final,
k) if upon transfer he/she does not report for duty within the legally-stipulated period without just cause – as of the date on which he/she is required to report for duty,
l) if he/she receives an evaluation of "unsatisfactory" twice consecutively – as of the date on which the final resolution on evaluation becomes effective,
m) in other cases specified by law.

ANNEX XXIII NAOS system consists of the following interconnected systems

name of the system	technology	Purpose of the system	status	technological upgrade
Web 2010 System	**oracle U.S.A.** **Microsoft U.S.A.** **adobe U.S.A.**	system for delivery, collection of reports on suspicious and cash transactions, transferring cash across the border	version 4.23 operational	technological upgrade needed: 1. Adobe master collection cs4 2. Microsoft visual studio
oracle databases system and data analysis tools	**oracle U.S.A.**	system for collection, recording, storing and analysing data. fundamental technological basis of the complete NAOS system of oracle databases and analytical tools for data processing.	oracle 9i operational	technological upgrade of oracle 9i needed: 1. oracle 11g, 2. analytical tools for data processing .
i2 analyst notebook	**IBM i2 U.S.A.**	system for visualization and analytical processing of cases.	version 6.0 operational	a technological upgrade to the version 8.0 needed which will enable;: 1. work with ibridge system for connecting and collecting data from the oracle database. 2. work with the ixa system for connecting and gathering information from different sources and locations
ViewWise	**computhink U.S.A.**	system for collecting, storing, managing cases of the anti-money laundering office	version 7.0 operational	a technological upgrade to the version 7.1 needed as well as transition from client server architecture to web based architecture.

ANNEX XXIV Training supplied to AMLO staff

2008

- The AMLO has organised several training for inspectors of the AMLO, in terms of using IT tools, and a seminar on the new legislation in the area of money laundering and terrorist financing;
- The AMLO organised a seminar for inspectors of supervisory authorities (Tax Administration, Financial Inspectorate, Customs Administration, Financial Police, CNB, HANFA) on the new legislation in the area of money laundering and terrorist financing;
- In cooperation with the Chamber of Commerce and CNB, seminar for Banks on the new legislation in the area of money laundering and terrorist financing;
- In cooperation with the Chamber of Commerce and HANFA, seminar for capital market participants on the new legislation in the area of money laundering and terrorist financing;
- In cooperation with the tax administration, seminar for the casinos on the new legislation in the area of money laundering and terrorist financing;
- In cooperation with the Croatian Association of auditors, accountants and tax consultants, seminar for auditors, accountants and tax advisers about the new legislation in the area of money laundering and terrorist financing;
- Participation of the AMLO representatives in the Criminal Police seminar in relation to financing of terrorism;
- The participation of representatives of the AMLO in the Judicial Academy seminars for prosecutors and judges on the issue of money laundering.

2009

- Seminar for analysts of financial intelligence units held in Tirana from 9 to 13 November 2009 – two representatives;
- National experts workshop on the Comprehensive approach to cyber security held on 23 and 24 November 2009 – three representatives;
- Seminar within the framework of the MATRA project – the Reorganisation of the Crime Investigation Police held at the premises of the Police Department Headquarters of the Croatian Ministry of the Interior on 10 and 11 November 2009 – one representative;
- Training relating the use of the Dow Jones Watch list – six representatives;
- Training relating to the use of FIU.NET – four representatives.

2010

- Education on World-Check database, January 2010 - 12 representatives;
- Project ILECUs Seminar on Marketing in international police cooperation, 21-22 January 2010 – 2 representatives;
- Project ILECUs Seminar on IT, EU investigative methods and analysis 26 - 28 January 2010 – 2 representatives;
- TAIEX Seminar on the Implementation of Regulation (EC) No 1889/2005 of the European Parliament and of the Council of 26 October 2005 on controls of cash entering or leaving the Community, Zagreb, 22 February 2010 - 5 representatives;
- TAIEX Seminar on the Responsibility of Lawyers and Notaries Public in Recognizing and Reporting Suspicious Transactions, Zagreb, 16 April 2010 - 6 representatives;
- Seminar on the work of Europol, Ministry of the Interior, Zagreb, 2 June 2010 – 8 representatives;
- OLAF Seminar on Financial Investigations and EU funds, Zagreb, 14-18 June 2010 – 2 representatives;
- Seminar on Financial Investigations - Matra Project, Ministry of the Interior, 16-18 June 2010 – 2 representatives;

- Seminar for accountants, 28 – 29 June 2010 – 3 representatives;
- Seminars on combating corruption – basic, advanced and training for trainers, Zagreb, June 2010 – 3 representatives;
- Round table on IPA 2007 project "Strengthening capacities of USKOK" – inter-agency cooperation, 7 September 2010 – 2 representatives;
- Seminar on OLAF investigations 6-7 October 2010, Zagreb, 2 representatives;
- Seminar on AML/CFT for banks and housing savings banks, 15 October 2010 – 2 representatives;
- Round table on IPA 2007 project "Strengthening capacities of USKOK", 8 - 9 November 2010 – 2 representatives;
- Seminar on reporting to senior officials - Matra Project, Ministry of the Interior,18 November 2010 - 2 representatives;
- TAIEX Seminar on AML/CFT – experience of EU banks, 19 November 2010 – 6 representatives;
- OESS Workshop on Public-Private Partnership in South-East Europe on suppression of financing of terrorism and violent extremism and radicalism, Sarajevo, 8 - 10 December 2010 - 1 representative;
- World Bank Seminar for FIU analysts, Paris, 6 - 9 December 2010 - 2 representatives.

2011

- Seminar on implementation of new Criminal Procedure Code, 27 – 28 January 2011, Zagreb – 2 representatives;
- Seminar on irregularities and fraud within the framework of AFCOS network (IPA project with Romanian experts) 1 – 2 March 2011, Zagreb – 1 representative;
- TAIEX seminar on suppression of corruption and special investigative measures, 2 – 3 March 2011, Zagreb– 2 representatives;
- Seminar on IT support for monitoring the implementation of measures from revised Action plan for the Strategy of suppression of corruption, 16 – 17 March 2011, Zagreb – 1 representative;
- Cybercrime workshop on criminal money flows on Internet, 17 – 18 March 2011, Belgrade – 1 representative;
- Study visit to Romanian DLAF, 20 – 26 March 2011, Bucharest – 1 representative;
- Conference on achievements and challenges in protecting EU's financial interests in the Republic of Croatia, 27 May 2011, Zagreb – 1 representative;
- Seminar on proactive approach to prevention, detection and investigation of corruption and organised crime, 6-7 June 2011, Zagreb– 2 representatives – 1 representative;
- Workshop on strategy to combat economic crime, 28-30 June 2011, Zagreb – 1 representative;
- Seminar "The Nexus of Terrorism", 28-30 June 2011, Mali Lošinj – 1 representative;
- Regional workshop on countering terrorist financing, 29-30 June 2011 – 1 representative;
- Seminar on risk assessment, 6th July 2011, Zagreb – 2 representatives;
- Seminar on pro-active approach in prevention, detection and investigation of corruption and organised crime, 11-12th July 2011, Zagreb – 2 representatives;
- Strategic Analysis Course, 12-15th September 2011, Doha, Qatar – 1 representative;
- Sub-regional workshop on Preventing and Countering the Financing of Terrorism, 27-29th September 2011, Moldova – 1 representative;
- Seminar on credit checks of business entities, 20th September 2011, Zagreb – 2 representatives;
- Seminar on payment transactions to abroad, 12th October 2011, Zagreb – 1 representative;
- Seminar on project cycle management I, 3-4th November 2011, Zagreb – 1 representative;
- Seminar on establishment and managing international joint investigation teams, 9-10th November 2011, Zagreb – 2 representatives;
- Seminar on IPA, 14-15th November 2011, Zagreb – 1 representative;
- Seminar on project cycle management II, 16-17th November 2011, Zagreb – 1 representative;

- ILEA Financial investigation techniques course, 21-25th November 2011, Budapest – 2 representatives.

2012

- Annual Workshop on AML/CFT, 23 January 2012., Zagreb – 12 representatives;
- Specialized workshops for non-financial sector, 24 January 2012., Zagreb – 12 representatives;
- Specialized workshops for casinos and other games of chance, 26 January 2012, Zagreb – 6 representatives;
- Advanced Training for AML/CFT for tax inspectors, 26 January 2012, Zagreb – 6 representatives;
- Workshop on the financial investigation unit (TAIEX), 2nd-3rd February 2012, Zagreb – 2 representatives ;
- Professional counselling of the professional criminalists associations, 2nd-3rd February 2012, Zagreb – 1 representative;
- Seminar on AML/CFT, financial investigations and confiscation of proceeds of crime, 6th-10th February 2012, Zagreb – 3 representatives;
- Seminar on the Protection of the financial interests of the European Union in the context of European enlargement policy, as part of the Romanian Sharing experiences with the Croatian authorities to combat irregularities and fraud in order to protect the financial interests of the EU, 12th-14th March 2012, Bucharest – 1 representative;
- Seminar on the detection and management of fraud concerning EU funds, as part of the Romanian Sharing experiences with the Croatian authorities to combat irregularities and fraud in order to protect the financial interests of the EU, 28th-29th March 2012, Zagreb – 1 representative;
- A seminar on the prevention of money laundering and terrorist financing, Croatia Chamber of Commerce, 4th-6th July 2012, Zagreb – 2 representatives;
- Seminar on financial investigations, ICITAP program, 27 - 31 August 2012, Zagreb – 4 representatives;
- Seminar on financial investigations, ICITAP program, 3 to 7 September 2012, Zagreb – 4 representatives;
- Workshop on Preliminary national risk assessment, the IMF, the 17th-21st September 2012th, Syracuse – 1 representative.

ANNEX XXV Customs Service Act

Article 18

(1) When authorised customs officers exercise supervision over enforcement of law and other executive regulations, exercise customs control, control of special taxes, prevent and detect the acts of offences and criminal acts under this Act and other laws, observing in their implementation the regulations on safety of air, maritime, inland waterway, railway and road traffic they shall also have the authority to:

1. follow, stop, inspect and search a vehicles, means of conveyance and goods,
2. check identity of a person,
3. inspect a person,
4. inspect and search business premises, facilities, documentation, as well as examine the authenticity and veracity of documents presented in the customs procedure,
5. temporarily seize the items and documents,
6. temporarily restrict the freedom to move,
7. summon,
8. collect, process, record and use personal and other data,
9. use means of coercion .

(2) Authorised customs officers shall be entitled to use coercive means only if allocated to a position determined as such by the Ordinance on internal order and if they passed the exam in accordance with prescribed training programme.
(3) Authorised customs officers who are appointed as investigators shall be entitled to conduct evidence recovery operations conferred by the State Attorney Office under the Criminal Procedure Act and rules of their profession.
(4) The training programme for authorised customs officers referred to in paragraph 2 of this Article shall be enacted by the Government.
(5) The manner of acting and use of coercive means shall be stipulated in the ordinance by the Minister of Finances on proposal of the director of Customs Administration.

Article 19

Authorised customs officers, when fulfilling duties referred to under Article 18 of this Act may use technical equipment, detection dogs and official vehicles and crafts with illumination and sound signals in accordance with the road traffic safety and maritime and inland waterway navigational safety regulations.

Article 20

(1) Authorised customs officers referred to under Article 18, paragraph 2 of this Act shall be entitled to carry firearms and ammunition on the entire customs territory of the Republic of Croatia.
(2) Authorised customs officers referred to under Article 18, paragraph 2 of this Act shall be entitled to carry firearms and ammunition while fulfilling the duties in official customs uniform, and exceptionally in civilian clothing, by the order of the superior, should justified reasons therefor prevail.
(3) The manner of carrying and use of firearms shall be stipulated in the Ordinance by the Minister of Finances.
(4) The type of firearms and ammunition used by authorised customs officers referred to in Article 18, paragraph 2 of this Act shall be stipulated by the Government in the Regulation.

Article 21

(1) Authorised customs officers shall be entitled to inspect the persons in cross-border traffic and to inspect and search the luggage and other items that such persons carry therewith. Such actions shall also involve the right of checking the identity of persons.
(2) Identity check of a person shall be conducted by consulting his/her passport, personal identity card or other public document containing photograph.
(3) On the occasion of checking the identity of a person, the authorised customs officer shall inform a person of the reasons of identity check thereof.
(4) The actions referred to in paragraph 1 of this Article shall also involve the right to temporarily restrict freedom of movement, pending completion of statutory customs operations, or if the offence perpetrated by violating the customs or tax regulations was committed or attempted, but for no longer than six hours. If there are reasons for temporary restriction of freedom of movement for a period exceeding six hours, competent police department shall be notified without delay.
(5) If the reason of temporary restriction of freedom of movement is the committing or attempt to commit the offence stipulated by other laws or by the criminal act, the competent police department shall be notified without delay.
(6) Authorised customs officers referred to in Article 18, paragraph 2 of this Act shall be entitled to inspect persons, inspect and search the luggage and other items that such persons carry therewith on the entire customs territory of the Republic of Croatia, if there are grounds for suspicion of committing the customs or tax offence or criminal act.
(7) Inspection of a person referred to under paragraph 1 of this Article, shall above all involve the inspection of anything such a person carries on his/her body or along with, whereby it shall be established whether he/she has therewith or thereon the goods which are the object of violation of customs or other regulations the conducting of which falls within the competence of Customs Administration or which are the object of criminal act. The inspection may only be conducted by authorised customs officers of same sex as a person who is subject to inspection, while inspection of a minor may only be conducted in the presence of his/her parents or tutors, while in their absence or refusal to attend the inspection, in the presence of social care worker.
(8) If there is a justified suspicion that goods which are the object of customs or tax offence pursuant to provisions the implementation of which falls within the competence of Customs Administration, or the object of criminal act, are hidden in body of a person, the carrying out of physical examination shall be entrusted to a physician of the public health service.
(9) If during inspection or search of goods, mean of transport or person, goods are found the trade in which is banned or restricted, and those are unlawfully conveyed into or from the customs territory of the Republic of Croatia, they shall be seized temporarily. The persons with who those have been found shall temporarily be subject to restricted freedom of movement, whereby the competent police department shall be notified immediately thereof.
(10) Should domestic or foreign instruments of payment be found with a person referred to in paragraph 1 of this Article in amounts exceeding those authorised, a procedure shall be undertaken in compliance with the foreign exchange and other regulations.
(11) Authorised customs officer shall issue confirmation of receipt upon temporary confiscation of an item. The receipt shall specify all the characteristics of the temporarily confiscated item which make it differ from other items as well as data on a person from which an item has been confiscated.
(12) The provisions of this Article shall also apply to driving personnel, the crew of transport vehicles, and to other persons subject to enforcement of customs control.

Article 22

(1) Authorised customs officers, for the purpose of detecting the violations of customs and tax regulations the implementation of which falls within the competence of Customs Administration shall on the entire customs territory of the Republic of Croatia be entitled to the following:

1. follow and arrest any transport and conveyance vehicle,
2. inspect and search anywhere a transport and conveyance vehicle,
3. control the designated use of motor fuel in means of transport, work devices and machinery.

(2) The persons subject to measures referred to in paragraph 1 of this Article shall stop at the place designated by authorised customs officer by showing prescribed signs in a manner and according to procedure prescribed by the ordinance of the Minister of Finances in agreement with the Minister of Internal Affairs. Upon request of the authorised customs officer, he/she must provide all the necessary data and show thereto the goods and products he/she transports or carries.
(3) The inspection of transport or conveyance mean implies sensory inspection of space and items therein.
(4) If at inspection of transport or conveyance vehicle, justified suspicion is ascertained in violating the customs or tax regulations the implementation of which falls within the competence of the Customs Administration, the authorised customs officer shall be entitled to conduct the search of all parts of the transport or conveyance mean, including the items therein, and using the technical aids he/she shall be entitled to dismantle individual parts of a transport and conveyance mean.
(5) Should it be established upon the inspection and dismantling of a transport or conveyance vehicle that there has been no violation of customs or tax regulations the implementation of which falls within the competence of the Customs Administration, the transport or conveyance vehicle shall be restored to the original state thereof.

Article 23

(1) Authorised customs officers, for the sake of detecting violations of customs and other regulations the conducting of which falls within the competence of customs service, shall on the entire customs territory of the Republic of Croatia be entitled to conduct the inspection and search of business premises and other business spaces in which the goods are produced, loaded, unloaded, transhipped or stored.
(2) Business premise within the meaning of paragraph 1 of this Article shall also mean the residential area indicated as registered office of the company or if used as business premises.
(3) The inspection of other premises and spaces may only be exercised on the basis of warrant of the judiciary authority.

Article 24

(1) Authorised customs officers shall be entitled to summon the participants in customs procedure and other persons for which it may be presumed to have access to information necessary for carrying out the tasks which fall within the scope of operations of customs service referred to in Articles 3, 9 and 10 of this Act, for the sake of providing oral or written information.
(2) Authorised customs officers shall be entitled to summon the participants in customs and tax procedure and other persons for whom it may be presumed to have access to information with the scope of discovering facts relevant for establishing the criminal liability for acts featuring violation of customs regulations, and other regulations falling within the competence of Customs Administration.
(3) The summon must specify the name, place and address of organisational unit of the Customs Administration, as well as the grounds for and place and time of summoning.
(4) A person who responded to the summons, but refused to give the information shall not be summoned again for the same reason.

ANNEX XXVI AMLO Procedures of Work of Department for Financial and Non-Financial Institutions Targeted Supervision

3.4. Request to carry out targeted supervision of reporting entities,

While carrying out the responsibilities of the Department of financial and non-financial institutions (performing indirect supervision, coordination of supervision with the supervisory authority) Head of the Department can give proposals to the Head of Service for the carrying out of the targeted supervision of the reporting entity/ies by the supervisory authority (Article 85 of the Law), in order to check the application of the Law on Prevention of Money Laundering and Terrorist Financing and the regulations issued there under, as well as the assessment of exposure to money laundering or terrorist financing risk.

After receiving approval the Head of Department will appoint an inspector to make a submissions to conduct targeted supervision which will be referred to the competent supervisory authority for further action with reference to the provisions of Article 86th of the Law that implies informing the Office as soon as possible on the carried out inspections and measures taken, irregularities and other significant information identified during supervision.

If during supervision the existence of suspicion that suggest the connection between some transactions with money laundering or terrorist financing, the supervisory authority will in accordance with Art. 87. of the Law without any delay, notify the Office in the manner prescribed by art. 64. of the Law.

The supervisory bodies to which targeted surveillance are proposed are

- **Financial Inspectorate** for reporting entities under Art. 4. para.2. point. 5., 6., 12., 14., 15. c), d), e), f), g), j), k), l), m), n), point. 16. of the Law – point. 5 companies performing certain payment operations services, including money transfers; point 6.Croatian Post Inc; point 12.authorised exchange offices; point. 14.pawnshops; point 15. c) payment instruments issuance and management (e.g., credit cards and traveler's cheques), d) issuance of guarantees and security instruments, e) investment management on behalf of third parties and providing advisory thereof, f) rental of safe deposit boxes, g) credit dealings intermediation, j) trusts or company service providers, k) trading precious metals and gems and products made of them, l) trading artistic items and antiques, m) organizing or carrying out auctions, n) real-estate intermediation. Point 16. legal and natural persons performing matters within the framework of the following professional activities: a) lawyers, law firms and notaries public, b) auditing firms and independent auditors, c) natural and legal persons performing accountancy and tax advisory services.

- **Tax administration** for reporting entities under Art. 4. para.2. point. 13. of the Law 13. organizers of games of chance: lottery games, casino games, betting games, slot-machine gaming, games of chance on the Internet and via other telecommunications means, i.e. electronic communications;

- **Croatian National bank** for reporting entities under Art. 4. para.2. point. 1., 2., 3., 4. and 11. of the Law – point. 1. banks, branches of foreign banks and banks from member-states authorized for a direct provision of banking services in the Republic of Croatia; point 2. savings banks; 3. housing savings banks; 4. credit unions; point 11. companies for the issuance of electronic money, branches of companies for the issuance of electronic money from member-states, branches of companies for the issuance of electronic money from third countries and companies for the issuance of electronic money from member-states authorized to directly render services of issuing electronic money in the Republic of Croatia;

- **Croatian agency for Supervision of Financial services** for reporting entities under Art. 4. para.2. point. 7., 8., 9., 10. and 15.a), b), h), i) of the Law - point. 7. investment funds management companies, business units of third countries management companies, management companies from member-states which have a business unit in the Republic of Croatia, i.e. which are authorized to directly perform funds management business in the territory of the Republic of Croatia and third parties which are allowed, in keeping with the law providing for the funds operation, to be entrusted with certain matters by the respective management company; 8. pension companies; 9.companies authorized to do business with financial instruments and branches of foreign companies dealing with financial instruments in the Republic of Croatia; 10. insurance companies authorized for the performance of life insurance matters, branches of insurance companies from third countries authorized to perform life insurance matters and insurance companies from member-states which perform life insurance matters directly or via a branch in the Republic of Croatia; point 15 a) factoring; point 15. b) leasing, point 15.h) insurance agents with entering into life insurance agreements, point 15. i) insurance intermediation with entering into life insurance agreements,

3.4.1. The purpose and objective
Direct (inspection) check:

- The application of certain provisions of the Law and the regulations issued pursuant to the Law
- Application of the provisions of the Law and the regulations issued pursuant to the Law at those reporting entity where irregularities have been detected

3.4.2. Connections with other processes
The process of registration of the acts, process of dispatching and archiving of the case file.

ANNEX XXVII CNB: Guidelines for the implementation of the Anti-Money Laundering and Terrorist Financing Law with respect to credit institutions, credit unions and electronic money institutions

Pursuant to Article 88 of the Anti-Money Laundering and Terrorist Financing Law (Official Gazette 87/2008 and 25/2012) and Article 43, paragraph (2), item (9) of the Act on the Croatian National Bank (Official Gazette 75/2008), the Governor of the Croatian National Bank has issued Guidelines for the implementation of the Anti-Money Laundering and Terrorist Financing Law with respect to credit institutions, credit unions and electronic money institutions.

1 Introductory provisions

1.1 Purpose and applicability of the Guidelines

For the purpose of a uniform application of the provisions of the Anti Money Laundering and Terrorist Financing Law (hereinafter: the Law) and pursuant to the regulations adopted on the basis thereof, the Croatian National Bank (hereinafter: the CNB), as the competent supervisory authority, hereby issues these Guidelines for the implementation of the Anti Money Laundering and Terrorist Financing Law with respect to credit institutions, credit unions and electronic money institutions (hereinafter: the Guidelines).

The Guidelines shall apply to the following obligated persons referred to in Article 4 of the Law (hereinafter: obligated persons), supervised by the CNB:

1. banks, Member States' bank branches, branches of third-country banks, and banks from Members States which are authorised for a direct provision of banking services in the Republic of Croatia;
2. savings banks;
3. housing savings banks;
4. credit unions; and
5. electronic money institutions, branches of Member States' electronic money institutions, branches of third-country electronic money institutions and electronic money institutions from Member States which are authorised for a direct provision of electronic money issuance services in the Republic of Croatia.

Being a part of the financial system which may be used for illegal purposes and through which money laundering and terrorist financing activities may be carried out, obligated persons are exposed to various kinds of risk (reputation[1], legal[2] and operational risks[3]) that can threaten their stability.
In order to reduce the exposure to the reputation, legal and operational risks, and particularly the risk of the financial system abuse by using various money laundering and terrorist financing methods and techniques, obligated persons should effectively apply the measures laid down in these Guidelines.

1.2 Money laundering
1.2.1 Money laundering definition

[1] Reputation risk is defined as the risk of a loss of trust in the integrity of an obligated person, caused by adverse public opinion on the obligated person's business practices and connections, regardless of whether there are any grounds for such a public opinion or not.
[2] Legal risk relates to the possibility that a legal action instituted against an obligated person, and contracts concluded or business decisions taken by that obligated person, which are found to be unenforceable, might adversely affect the obligated person's business or financial position.
[3] Operational risk is defined as the risk of loss resulting from inadequate or failed internal processes, people or systems, or external events, including a legal risk.

Money laundering means the undertaking of actions aimed at concealing the true source of money or other property suspected to have been obtained in an illegal manner in the country or abroad, including:
1. the conversion or any other transfer of money or other such property;
2. the concealment of the true nature, source, location, disposition, movement, ownership or rights with respect to money or other such property; and
3. the acquisition, possession or use of money or other such property.

1.2.2 Money laundering stages

The process of money laundering generally involves the following three stages:

1. Placement stage
Illicitly acquired funds are initially entered into the financial system. At this stage, the "dirty" money is most visible and easy to detect.

2. Layering stage
At this stage, the funds are entered into financial flows, where a number of complex transactions are used to disguise the origins or owners of illicitly acquired funds. The detection of the "dirty" money becomes more difficult.

3. Integration stage
At this stage, the "dirty" money is re-entered into the legal financial flows and included into other financial system assets of a country, which makes its detection almost impossible.

1.2.3 Money laundering methods

Due to technological progress, an increased number of sophisticated and complex methods are used to conceal the origins of illicitly acquired funds.

Of a large number of methods, only a few most commonly used ones are described, aimed at circumventing the money laundering detection and prevention system:

1. Structuring - the breaking of larger amounts of cash over a reporting limit into cash transactions of smaller amounts and their placement into the financial system. The smaller cash amounts are most commonly deposited by a rather large number of persons, in order to avoid detection, or evade the obligation to report on cash transactions above a certain amount and the customer identification obligation.
2. Multiple transactions - the same person carries out two or more transactions in one day, where the total amount of transactions in a day exceeds the prescribed limit for customer identification and identity verification, or notification of the Anti-Money Laundering Office (hereinafter: the Office).
3. Purchase/sale of foreign currency - illicitly acquired funds are used for the purchase of foreign currency which is then transferred to bank accounts held with off-shore financial centres.
4. Using nominal representatives - the most commonly used method at the placement stage. A person intending to enter dirty money into the financial system can try to conceal the origin of the illicit funds, by including a nominal representative, such as a family member, a friend or a business acquaintance enjoying the trust of the community.

The most common methods of laundering money acquired through some of the so-called predicate offences are the following:

1. the use of various forms of companies and foundations, particularly shell companies, established in countries with no strict regulations on the prevention of money laundering and identification of its true owners;

2. the use of the services of various legal and/or financial experts, particularly lawyers, who establish companies, open bank accounts, make cash transfers, buy assets and perform other tasks on behalf of their clients.

3. the use of domestic credit/financial institutions: enhanced due diligence is conducted only in the case of politically exposed foreign persons; for that reason, politically exposed persons use accounts in banks having their seat in a country of their residence, either at the layering stage or by returning the cash to a "domestic" bank after it has been "laundered" abroad;

4. the use of foreign/offshore jurisdictions, particularly the use of several foreign/offshore jurisdictions in a way that, for example, a bank account in one country is owned by a company with a seat in another country, where the "owner" of that company has a seat in a third country, etc.; an increased number of foreign/offshore jurisdictions involved in the scheme, hinders the performance of legal actions for identifying the offence and its perpetrators by the criminal prosecution authorities in the country where the predicate offence has been committed;

5. the use of trustees - the use of family members, friends or close business associates, carrying out transactions in their own name, but for the account of a politically exposed person;

6. the use of cash - given its anonymous character, i.e. given no written record of its transfer, cash is attractive to money "launderers"; in the case of politically exposed persons, another advantage is the exemption of "diplomatic baggage" from customs control and its use for the transfer of cash across the border.

1.3 Terrorist financing

1.3.1 Terrorist financing definition

In the broadest sense, the term terrorism includes any use of violence for the purpose of achieving political goals. The term 'terrorist financing" means the provision or collection of, as well as an attempt to provide or collect legal or illegal funds by any means, directly or indirectly, with the intention to be used, or in the knowledge that they are to be used, in full or in part, for the commitment of a terrorism offence by a terrorist or by a terrorist organisation.

A terrorist financing risk is the risk that the financial system might be abused for terrorist financing purposes, or that a legal relationship, a transaction or a product might be directly or indirectly used for terrorist financing purposes.

In contrast to money laundering, which is always preceded by an unlawful act, terrorism may be financed from revenues generated through legal activities (of humanitarian organisations or various associations, or from donations, etc.). This circumstance greatly complicates the detection of terrorist financing, particularly as the amounts of transactions used for terrorist financing are often lower than the prescribed limit for reporting to the Office. The measures taken to prevent money laundering are insufficient to combat terrorist financing and have to be supplemented by special measures prescribed by competent international bodies.

1.3.2 Terrorist financing methods

The characteristics of terrorist financing differ from those of money laundering, so it is difficult to assess the associated risk without a complex set of indicators of the methods and techniques that are used for terrorist financing.
As the funds used to finance terrorist activities may be derived either from criminal activities or from legal sources, the nature of the funding sources may vary according to the type of terrorist

organisation. Where funds are derived from criminal activity, then the risk-based approach used to identify money laundering may also be appropriate
for terrorist financing.

Where the funds used for financing terrorist activities are from legal sources, it is more difficult to establish that they are used for terrorist purposes. Moreover, preparations for terrorist activities can be public and overt, such as the purchase of materials and services (e.g. common chemical products, motor vehicles, etc.).

However, in the context of terrorist financing, the responsibility of obligated persons is not to identify a criminal offence, or intended terrorist financing, but to report suspicious activities. The Office and criminal prosecution authorities are responsible for a further investigation into the matter and for establishing a potential connection with terrorism.

Given the international character of terrorist financing and the lack of generally accepted typologies, i.e. methods and techniques used for terrorist financing, obligated persons are instructed to monitor and report to the Office transactions with countries identified by credible sources as countries that finance or support terrorist activities and in which identified terrorist organisations are known to operate.
The term "credible sources" refers to information provided by well-known bodies, that are generally regarded as reputable and that make such information publicly and widely available. In addition to the Financial Action Task Force and regional bodies operating in accordance with the FATF, such sources may include, but are not limited to, international bodies such as the International Monetary Fund, the World Bank and the EGMONT Group, as well as relevant national government bodies and non-governmental organisations. Information provided by these credible sources does not have the force of law or regulation and should not be viewed as an automatic determination that something poses a higher risk.

The method of monitoring and reporting such transactions is defined in Articles 42 and 43 of the Law.

As the prevention of money laundering and the prevention of terrorist financing have similar objectives, the basic features of both approaches produce synergistic effects. In both cases, efforts are made to conceal funds and financial transactions by hiding the sender and the recipient of the funds and concealing their mutual connection.

2 Legislative framework for the prevention of money laundering and terrorist financing

2.1 The Law and subordinate legislation

The legislative framework for the prevention of ML/TF in the Republic of Croatia comprises the Law, which is fully in line with the Directive 2005/60/EC of the European Parliament and of the Council on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing (Official Journal of the European Union L 309/15), the so-called Third Directive, and ordinances of the Ministry of Finance of the Republic of Croatia, enacted in accordance with the Law:

1. Ordinance on the determination of conditions under which obligated persons identify customers as customers who pose a negligible risk in terms of money laundering or terrorist financing (Official Gazette, 76/2009);

2. Ordinance on the content and type of data on the payer, accompanying electronic funds transfer, the obligations of payment service providers and on exemptions from the obligation to collect data in funds transfer (Official Gazette, 1/2009);

3. Ordinance on the obligation to report cash transactions in the amount of HRK 200,000.00 or more to the Anti-Money Laundering Office, and on conditions under which obligated persons are not required to report cash transactions of certain customers to the Anti-Money Laundering Office (Official Gazette 1/2009);

4. Ordinance on the obligation to report suspicious transactions and persons to the Anti-Money Laundering Office (Official Gazette 1/2009);

5. Ordinance on conditions under which persons subject to the Anti Money Laundering and Terrorist Financing Law may outsource customer due diligence measures to third parties (Official Gazette 76/2009);

6. Ordinance on the manner and time limits for reporting suspicious transactions and persons to the Anti-Money Laundering Office and on the keeping of records by lawyers, law firms, public notaries, audit firms and independent auditors, as well as legal and natural persons engaged in accounting and tax counselling activities (Official Gazette 1/2009);

7. Ordinance on the control of domestic and foreign currency cash taken in and out of the country across the state borders (Official Gazette 1/2009);

8. Ordinance on the manner and time limits for submitting data on criminal activities of money laundering and terrorist financing to the Anti-Money Laundering Office (Official Gazette 76/2009);

9. Ordinance on the manner and time limits for submitting data on misdemeanour proceedings to the Anti-Money Laundering Office (Official Gazette 76/2009).

2.2 Criminalisation of money laundering and terrorist financing activities

Money laundering offences are criminalised under Article 279 of the Criminal Code (Official Gazette 110/1997, 27/1998, 129/2000, 51/2001, 111/2003, 105/2004, 84/2005, 71/2006 and 152/2008), which provides that a criminal offence of money laundering is committed by a person who, in banking, financial or other economic operations, invests, takes over, exchanges, converts or otherwise conceals the true source of money, objects, rights or pecuniary gains, which he/she knows to be acquired through a criminal offence.

Terrorist financing is criminalised as a specific criminal offence of the planning of criminal offences against the values protected by international law, referred to in Article 187a of the Criminal Code, providing that a criminal offence is committed by a person who, directly or indirectly, provides or raises funds with the intention of using them, entirely or in part, for the perpetration of, among other things, a crime of terrorism, referred to in Article 169, a crime of incitement to terrorism, referred to in Article 169a, and a crime of recruitment and training for terrorism, referred to in Article 169b.

Pursuant to a new Criminal Code (Official Gazette 125/2011), entering into force on 1 January 2013, money laundering offences and terrorist financing offences are criminalised under Articles 265 and 98 respectively.

Article 265 provides that whoever invests, takes over, converts or exchanges pecuniary gains acquired through a criminal offence with the intention of concealing their illicit origin shall be punished by imprisonment for six months to five years.

Article 98 provides that whoever directly or indirectly, provides or raises funds with the intention of using them, or knowing that they are to be used, entirely or in part, for the perpetration of one or several criminal offences referred to in Article 97 (terrorism), Articles 99 (public incitement to terrorism) to 101 (training for terrorism), Article 137 (abduction), Article 216, paragraphs (1) to (3)

(destruction or damage of public utility installations), Article 219 (abuse of radioactive substances), Article 223 (attack on an aircraft, a ship or an immovable device), Article 224 (endangering the safety of traffic by a dangerous act or means), Article 352 (murdering a person under international protection) and Article 355 (threatening a person under international protection) of that Code, or other criminal offences aimed at causing death or inflicting a serious bodily injury to a civilian or another person not actively participating in the armed conflict, provided that the purpose of such an act is to intimidate the population or coerce a state or an international organisation into doing or not doing something, shall be punished by imprisonment for one to ten years. The same punishment shall be inflicted on whoever provides or raises funds with the intention that they are used, or knowing that they are to be used, entirely or in part, by a terrorist or a terrorist association.

3 Measures to be carried out by obligated persons for the purpose of the ML/TF prevention

3.1 Organisation of an obligated person's AML/TF system

3.1.1 Appointment of an authorised person

Pursuant to Article 44 of the Law, an obligated person shall appoint an authorised person and one or several deputies to the authorised person. The authorised person and his/her deputies are persons authorised and responsible for carrying out the measures and actions aimed at preventing and detecting ML/TF within the obligated person. The authorised person's deputy replaces the authorised person during his/her absence in the performance of the activities prescribed by Article 46, paragraph (1) of the Law, and carries out other tasks under the Law, if so provided by an internal bylaw.

Pursuant to Article 45 of the Law, an obligated person shall ensure that the tasks of the authorised person or the authorised person's deputy can only be carried out by a person who meets the following requirements:

1. that the person is employed at a position within the obligated person's organisational scheme, which enables the person to carry out the tasks prescribed by the Law and regulations adopted on the basis thereof in a quick, efficient and timely manner, to be independent in his/her work and to communicate directly with the management board;

2. that the person is not undergoing criminal proceedings, i.e. the person was not convicted of a crime against the values protected by international law, safety of payment operations and arrangements, credibility of documents, against property and the official duty for a period of 5 years from the finality of the judgement by which the person had been convicted, excluding the time of serving a sentence;

3. that the person is adequately professionally trained to carry out tasks in the field of the ML/TF prevention and detection, and has the abilities and experience necessary to perform the functions of an authorised person; and

4. that the person is well familiarised with the nature of the obligated person's operation in the fields exposed to the ML/TF risk.

In addition, pursuant to Article 47 of the Law, an obligated person shall ensure the following conditions to the authorised person and the deputy:

1. unrestricted access to all data, information and documentation necessary for the ML/TF prevention and detection;
2. adequate authorisation for an efficient performance of the authorised person's tasks prescribed by the Law;
3. adequate personnel-related, material and other working conditions;
4. adequate premises and technical conditions, which will guarantee an appropriate level of protection for confidential data and information available to the authorised person and the deputy under the Law;

5. adequate IT- support enabling ongoing and safe monitoring of the activities in the field of the ML/TF prevention and detection;
6. regular professional training and development in the ML/TF prevention and detection;
7. replacement of the authorised person during his/her absence.

Equally, pursuant to Article 47, paragraph (3) of the Law, an obligated person shall ensure that the persons performing the function of the authorised person or the deputy carries out his/her work and tasks as an exclusive full-time work duty, where the volume of tasks in the field of the ML/TF prevention and detection is permanently increased due to a large number of employees, the nature or scope of the obligated person's operations or for other justified reasons.

In such cases, the obligated person shall enable the authorised person to carry out his/her tasks as an autonomous organisational unit, directly accountable to the management board and organisationally segregated from other organisational units of the obligated person.

Those obligated persons who, on the basis of the number of their employees, the nature or scope of their operations or for other justified reasons, assess that the volume of their tasks in the field of the ML/TF prevention and detection has not permanently increased, may include the authorised person into another organisational unit, or may organise the carrying out of the authorised person's tasks in a way other than as an exclusive full-time work duty.

In any case, however, obligated persons shall ensure that the authorised person is employed at a position within the obligated person's organisational scheme, which enables the person to carry out the tasks prescribed by the Law and regulations adopted on the basis thereof in a quick, efficient and timely manner, to be independent in his/her work and to communicate directly with the management board;

Pursuant to Article 46 of the Law, the authorised person and the deputy shall be authorised to carry out all the measures and actions prescribed in this Law, notably as follows:
1. taking care of the establishment, operation and development of the ML/TF prevention and detection system within the obligated person;

2. taking care of the regular and timely provision of data to the Office, in accordance with the Law and the regulations adopted on the basis thereof;

3. taking part in the preparation of operational procedures and amendments thereto, and in the drafting of the obligated person's internal bylaws applicable to the ML/TF prevention and detection;

4. taking part in drawing up guidelines for conducting internal audits with respect to the ML/TF prevention and detection;

5. monitoring and coordinating the activities of the obligated person in the field of the ML/TF prevention and detection;

6. taking part in the establishment and development of IT support for carrying out the activities in the field of the ML/TF prevention and detection within the obligated person;

7. providing incentives and making suggestions to the management board for improvements in the ML/TF prevention and detection system;

8. taking part in the preparation of the professional training and development program for the obligated person's staff members in the field of the ML/TF prevention and detection.

An obligated person shall notify the Office of the appointment of an authorised person and the deputy immediately, but no later than 7 days from the appointment, or from a change of the authorised person's data.

3.1.2 Organisation of an AML/TF system

Pursuant to Article 46, paragraph (1), item (1) of the Law, an authorised person and the deputy shall, among other tasks, take care of the establishment, operation and development of the ML/TF prevention and detection system within the obligated person.

Moreover, Article 47, paragraph (2) of the Law prescribes that internal organisational units and the management board are obliged to ensure that the authorised person and the deputy have assistance and support during the performance of the tasks prescribed by the Law and regulations adopted on the basis thereof, and to inform them permanently of all the activities which were, or might be related to ML/TF. The manner of submitting the notifications and the course of cooperation between the authorised person and employees within other organisational units shall be prescribed in detail in the obligated person's internal bylaws.

In the process of establishing an AML/TF system, obligated persons should take account of the following:

1. the nature, scope and complexity of the obligated person's operations;
2. the diversity of the obligated person's operations, including geographical distribution;
3. the obligated person's customer, product and activity profiles;
4. the distribution channels used;
5. the volume and size of transactions;
6. the degree of risk associated with each area of the institution's operation;
7. the extent to which the institution is dealing with the customer directly or through intermediaries, third parties, correspondents, or using a non-face-to-face approach.

Based on the analysis of the above mentioned elements, obligated persons assess their own exposure to the ML/TF risk, in order to determine the level of complexity of the AML/TF system. The system complexity will be manifested in the manner in which an obligated person ensures the application of the provisions of the Law concerning: the authorised person and his/her deputy, internal bylaws, staff training and education, the obligation to conduct regular annual internal audits, data keeping, record keeping and the information system.

In order to ensure maximum efficiency of the established AML/TF system and the compliance of an obligated person's operations with the provisions of the Law, the system has to comply with the basic principles of the internal control system, and to ensure the following:

1. the application of an approach based on customer/product/transaction/country risks - an AML/TF system relying on the risk-based approach enables increased focus on an obligated person's customers/products/transactions that are perceived as more vulnerable to abuse in terms of ML/TF. Increased focus involves the application of more complex and intensive customer due diligence procedures, monitoring of customers' business relationships and implementation of other measures and activities provided by the Law, for the establishment or continuation of a particular relationship or for conducting transactions;
2. adequate professional training and education for all staff members involved in the AML/TF system - the continuous professional training and development ensures the compliance of an obligated person's operations with the provisions of the Law, enables staff members to be clearly familiarised with their powers, roles and responsibilities in the AML/TF system, and improves the obligated person's organisational culture;
3. adequate inclusion of the internal audit function (for some obligated persons, also external audit or external experts) - regular annual internal audits provide for a regular review of the

risk assessment and management processes relating to ML/TF , and efficiency of the established AML/TF system;

4. adequate inclusion of the compliance function into the AML/TF system - the inclusion of the compliance function enables continuous monitoring of the compliance of the obligated person's operations with the provisions of the Law and regulations adopted on the basis thereof, the estimation of effects of the relevant regulation changes on the obligated person's operations, and verification of the compliance of new products or procedures with the relevant laws and regulations;
5. adequate senior management involvement in the AML/TF system - strong senior management leadership in AML/TF is an important aspect of an efficient AML/TF system. Senior management must promote compliance with the regulations and ensure consistent application of the obligated persons' internal policies, procedures and other internal bylaws by all staff members within their responsibility;
6. an adequate reporting system - apart from the direct accountability of the authorised person to the obligated person's management board, it is necessary to establish the appropriate reporting lines, i.e. the way of communication between the authorised person and control functions, between the authorised person and senior management, between the authorised person and responsible persons in individual organisational units, e.g. offices, etc. The reporting system should, in addition to regular reporting, provide for timely notification of all relevant lines of responsibility of identified deficiencies in the AML/TF system, corrective actions taken and the persons determined and time limits set for their correction;
7. an adequate information system - the obligated person's information system must provide for prompt, timely and full reporting to the Office on the persons and transactions prescribed by the Law. Furthermore, the information system should be permanently improved and upgraded, in order to enable the consistent an simpler application of the legal regulations, by both the authorised person and his/her deputy and all staff members involved in the operational implementation of the Law.

3.1.3 Internal bylaw

Pursuant to Article 48 of the Law, obligated persons shall adopt internal bylaws prescribing measures, actions and procedures for the ML/TF prevention and detection in accordance with the Law and regulations adopted on the basis thereof.

The measures, actions and procedures to be prescribed by each obligated person in an internal bylaw, which arise from the provisions of Articles 7, 8, 32, 34, 41, 47 and 48 of the Law are the following:

1. An analysis, i.e. assessment of risk to rate the risks of:
   a) an individual group or type of customers;
   b) a business relationship; and
   c) a product or transaction;
2. Procedures for the implementation of customer due diligence measures:
   a) identifying the customer and verifying the customer's identity on the basis of documents, data or information obtained from a credible, reliable and independent source;
   b) identifying the beneficial owner of the customer and verifying the beneficial owner's identity;
   c) methods and procedures for obtaining information on the purpose and intended nature of the business relationship or transaction;
   d) methods and procedures for ongoing monitoring of the business relationship;
3. Procedures to determine whether a customer is a politically exposed person or not;
4. Policies and procedures for risks involved in a business relationship or transaction with customers who are not physically present:
5. A list of indicators for the detection of suspicious transactions and customers, in relation to which there are grounds for suspicion of ML/TF;

6. The manner of sending notifications and the course of cooperation between the authorised person and employees in other organisational units;
7. The responsibility of authorised persons in charge of the implementation of the Law in the case of the non-observance of the provisions of the Law and regulations adopted on the basis thereof, as well as the responsibility of all other obligated person's staff members taking part in the implementation of the Law and regulations adopted on the basis thereof.

In addition to the above mentioned, obligated persons should prescribe in their internal bylaws, according to their size and the nature and scope of their operations, the following measures, actions and procedures:

1. Monitoring procedures for customers or business relationships according to the established level of risk;
2. Enhanced customer due diligence procedures, i.e. procedures in the case:
   a) of establishing as correspondent relationship with a bank or other similar credit institution with a seat in a third country;
   b) of establishing a business relationship with a customer that is a politically exposed person; and
   c) when a customer is not physically present during the identification and identity verification procedures.
3. The manner of identifying and monitoring suspicious transactions and procedures applied by staff members upon detection of suspicious transactions;
4. The manner and dynamics of and responsibility of the authorised person and his/her deputy in reporting to the Office on the prescribed transactions and in the provision of other information and data to the Office;
5. The manner of and time limits for preparing a staff training and education program and the method of its implementation;
6. Record keeping: the manner of keeping data, retention periods, the content of records and data protection.

Staff members must be familiar with the provisions of internal bylaws and their impact on daily operations, in order to ensure consistent application of these provisions in practice and maximum efficiency of the staff members.

Obligated persons should ensure that the internal bylaws are easily accessible to the staff members e.g. at the obligated person's internal portal, and that the staff members are regularly informed of any amendments to these bylaws.

3.1.4 Producing a list of indicators

Pursuant to Article 41 of the Law, obligated persons are required to produce a list of indicators for the detection of suspicious transactions and customers in relation to which there are grounds for suspicion of ML/TF. When producing the list of indicators, obligated persons are required to take account of the specific features of their respective operations and characteristics of suspicious transactions referred to in Article 42, paragraph (7) of the Law. In the compilation of the list of indicators, obligated persons cooperate with the CNB.

When establishing the grounds for suspicion of ML/TF, obligated persons are required to use the list of indicators. Obligated persons must amend the list of indicators, which is an integral part of an obligated person's internal bylaw, and adapt it to the money laundering trends and typologies known to them, as well as to the circumstances stemming from the obligated person's operation.

3.1.5 Staff training and education

Pursuant to Article 49 of the Law, obligated persons are required to ensure regular training and education of all staff members involved in the tasks related to the ML/TF prevention and detection. Furthermore, the Law provides that the staff training and education should include the familiarisation with the provisions of the Law and regulations adopted on the basis thereof, with the obligated person's internal bylaws, and with international standards stemming from international AML/TF conventions, with guidelines and the list of suspicious transactions detection indicators, and with other tasks prescribed by the Law.

During the preparation of an annual staff training and education program, obligated persons should ensure that the program is appropriate to the type and scope of their operations and to the obligated persons' exposure to the ML/TF risk. In any case, the annual staff training and education program must enable the staff members to better understand their obligations with respect to AML/TF and their roles in the established AML/TF system, and with respect to the exposure of their operations to the ML/TF risk.

Obligated persons should educate their staff members on most of these topics through internally organised workshops, and should establish an efficient reporting and education system at the internal web portal, in the form of brief information, written materials and on-line education programs. Moreover, obligated persons should, in accordance with their abilities, refer the staff members to seminars organised by other domestic and foreign institutions for the purpose of acquiring new knowledge and experience.

The annual staff training and education program must cover all the staff members involved in the tasks related to the ML/TF prevention and detection. It is particularly important that the program should cover new staff members before they start interacting with customers. Hence, the ML/TF prevention and detection training should be an integral part of initial training and guidance programs for new staff members.

Obligated persons are required to prepare the annual staff training and education programs in the field of the ML/TF prevention and detection for the next calendar year by the end of the current year. The programs should be documented and must show which staff members will take part in a particular training program and in which time period.

Pursuant to Article 46, paragraph (1), item (8) of the Law, both the authorised person and his/her deputy shall take part in the preparation of a program. Moreover, the annual staff training and education program should be included in the audit program and evaluated within the regular annual internal audit procedure.

3.1.6 Internal audit

Pursuant to Article 50 of the Law, obligated persons are required to ensure that a regular internal audit of the performance of AML/TF tasks is carried out at least once a year and to inform the Office accordingly at request. The purpose of the regular internal audit is to detect and prevent irregularities in the implementation of the Law and to improve the internal system for detecting suspicious transactions and persons.

The regular internal audit obligation for credit institutions and electronic money institutions should be discharged by the internal audit function. As the said institutions are required to adopt audit programs for each area of internal audit, including the audit of the AML/TF system, they should ensure that this program is consistent with the size and volume of a given institution's operation, its risk profile and exposure to the ML/TF risk and that it is tailored to the specific characteristic of the ML/TF prevention system established within the institution.

The internal audit function is obliged to prepare a report on each completed audit, including the audit of the AML/TF system. Should the internal audit function, during the performance of internal audits,

detect deficiencies, irregularities or illegalities in the AML/TF system, it shall impose measures and set deadlines for their correction. The internal audit function shall submit the report to the Audit Committee, a member of the Management Board responsible for the audited areas of operation, the authorised person and the responsible persons of the organisational units competent for the audited areas of operation.

Credit unions are not legally obliged to establish an internal audit function and should therefore entrust the conduct of the regular annual audit of the performance of the AML/TF tasks to an audit firm that will carry out the audit of the annual financial statements in accordance with the legislation governing accounting and auditing, or, where appropriate, to a person with the title of an auditor, obtained in accordance with the law governing auditing.

3.1.7 Data retention and records keeping

3.1.7.1 Data retention

Pursuant to Article 78 of the Law, obligated persons are required to retain the data collected in accordance with the Law and regulations adopted on the basis thereof and the pertaining documentation for a period of ten years after the execution of a transaction, termination of a business relationship or a customer's access to a safe deposit box.

Furthermore, obligated persons are required to retain data and the pertaining documentation on an authorised person and the authorised person's deputy, the staff training and development and on the conduct of a compulsory internal audit for a period of four years after the appointment of an authorised person and the authorised person's deputy, the delivery of the staff training and education or the completion of the internal audit.

Obligated persons should additionally regulate the stated time limits prescribed by the Law in their internal bylaws. Obligated persons should also regulate in their internal bylaws the manner, form and place of retaining the data collected pursuant to he Law, data protection measures and procedures for data handling after the expiry of the retention period.

3.1.7.2 Secrecy of collected data and procedures

Pursuant to Article 75 of the Law, obligated persons and their staff members may not disclose the following information to a customer or a third party:

1. that the Office was, or will be supplied with a piece of data, information or documentation on the customer or a transaction referred to in Article 42, Article 54, paragraphs (1) and (2) and Article 59 of the Law;
2. that the Office has temporarily suspended the execution of a suspicious transaction, or has given instructions to this effect to the obligated person pursuant to Article 60 of the Law;
3. that the Office requested ongoing monitoring of a customer's financial operations pursuant to Article 62 of the Law; and
4. that pre-investigatory proceeding have been initiated, or might be initiated against a customer or a third party due to suspicion of money laundering or terrorist financing.

The data submitted in accordance with Article 42 of the Law are labelled as classified data for which an adequate secrecy degree is determined in accordance with Article 9 of the Data Secrecy Act (OG 79/2007). The secrecy degree RESTRICTED is assigned to information the unauthorised disclosure of which would be damaging to the functioning of state authorities and performance of their tasks which are of security interest to the Republic of Croatia.

The exchange of information collected in accordance with the Law between credit and financial institutions belonging to the same group in the country and abroad may only include statistical data,

e.g. the number of reported suspicious cash transactions, number of applications received by the Office, etc., but without indicating the identification data on persons or transactions.

3.1.7.3 Records keeping

Pursuant to Article 81, obligated persons are required to keep the following records:

1. records of customers, business relationships and transactions amounting to HRK 105,000.00 or more, regardless of whether the transaction is a single one or there are several, obviously interrelated transactions, amounting to a total of HRK 105,000.00 or more;
2. records of the data submitted to the Office on each cash transaction amounting to HRK 200,000.00 or more
3. records of transactions which the obligated person has not executed because the obligated person knew or suspected that the transactions were related to ML/TF, and which have been reported to the Office;
4. records of the supervisory bodies' inspections of classified data, with the indication of the name of the supervisory body, the name and surname of the authorised person who carried out the inspection and the date and time of the data inspection.

In addition, pursuant to Article 43 of the Law, obligated persons are required to analyse the background and purpose of complex and unusual transactions and to make a written record of the analysis results in order to make them available at the request of the Office
and other supervisory bodies.

Obligated persons should regulate in their internal bylaws the manner and form of keeping and accessing the records made in accordance with the Law.

3.1.8 Establishing an information system

Pursuant to Article 6, obligated persons are required to establish an information system adequate to their respective organisational schemes, in order to provide the Office with prompt, timely and complete information as to whether or not they maintain or have maintained a business relationship with a given natural or legal person, as well as to the nature of such a relationship.

Furthermore, pursuant to Article 47 of the Law, obligated persons are required to provide the authorised person and his/her deputy with adequate IT support to enable ongoing and safe monitoring of the activities in the field of the ML/TF prevention and detection;

In addition, pursuant to Article 46 of the Law, the authorised person and his/her deputy are authorised to take part in the establishment and development of IT support for carrying out the AML/TF activities.

In order to be able to provide the Office with prompt, timely and complete information as to whether or not they maintain, or have maintained a business relationship with a given natural or legal person, as well as to the nature of such a relationship, obligated persons should continuously improve their current information systems, so that they enable the staff to keep records of customers and to monitor the relationships with customers in a quick and efficient way, i.e. that the possibilities of updating, monitoring and searching customer data within the system are adequate for the processing and searching of high quantities of data in a short time. Consequently, obligated persons are encouraged to upgrade their information systems to include, e.g. differentiation between cash and cashless transactions, easier detection of suspicious transactions, monitoring of interrelated cash transactions, etc.

3.2 Risk assessment

Pursuant to Article 7 of the Law, obligated persons are required to carry out an analysis of the ML/TF risk and to use it for the assessment of the risks of a particular group or type of customers, business relationships, products or transactions with respect to a possible abuse related to money laundering and terrorist financing. Obligated persons are required to align the risk analysis and assessment, regulated by internal bylaws, with these Guidelines.

In addition to the risk-based approach, within which risk categories related to money laundering and terrorist financing are determined, these Guidelines also provide instructions for establishing policies and procedures aimed at reducing exposure to the money laundering and terrorist financing risks which may stem from new technologies enabling anonymity (electronic or Internet banking, electronic money, etc.).

The Guidelines also apply to all activities performed by obligated persons on the Internet, including all connected technologies enabling network access and open telecommunications networks, including direct telephone links, the World Wide Web and virtual private networks.

3.2.1 Risk-based approach[4]

The ML/TF risk is defined as the risk of abuse of the financial system by the customer for ML/TF and the risk that some business relationship, transaction or product may be used directly or indirectly for ML/TF.

In accordance with the Law, obligated persons independently assess the exposure of their customers or business relationships, transactions and products to the ML/TF risk. The categories, criteria and elements of risks defined in these Guidelines indicate potential ML/TF risks. The initial assessment of a customer made by an obligated person should be based on these risk categories and criteria, while individual risk elements may increase or decrease the initial assessment of the exposure.

The purpose of introducing the risk-based approach is to ensure that the AML/TF measures applied by obligated persons are proportionate to the identified risk. This approach provides for determining potential ML/TF risks and enables obligated persons to focus on those customers, business relationships, transactions or products that pose the highest potential risk.

Obligated persons must be able to prove that the level of due diligence measures applied is appropriate with respect to the ML/TF risk.

3.2.2 The ML/TF risk assessment

3.2.2.1 Risk categories, criteria and variables

Risk categories
When analysing and assessing the ML/TF risks, obligated persons classify their customers, business relationships, transactions or products into the following categories:

1. **low risk;**
2. **moderate risk; and**
3. **high risk.**

Risk criteria
The most commonly used risk criteria are:

1. country or geographic risk;
2. customer risk; and

[4] The risk-based approach is dealt with in the FATF document: *Guidance on the Risk-based Approach to Combating Money Laundering and Terrorist Financing*. http://www.fatf-gafi.org/dataoecd/43/46/3896057.pdf

3. product/transaction/business relationship risk.

Risk variables
An obligated person's methodology based on risk analysis and assessment may take into account risk variables which are specific to a particular customer, business relationship, product or transaction and which may increase or decrease the risk. The risk variables include:

1. **The purpose of an account or a business relationship —** accounts opened to carry out common, low-value customer transactions may pose a lower risk than accounts opened to carry out large cash transactions by a previously unknown customer.
2. **The level of assets or the size of transactions** — unusually high levels of assets or unusually large transactions compared to what might reasonably be expected of customers with a similar profile may indicate that a customer, not otherwise seen as higher risk, should be treated as such.
3. **The level of regulation** or another oversight or governance regime to which a customer is subject — a legally regulated financial institution in a country with a satisfactory anti-money laundering regime poses less risk than a customer that is unregulated or subject only to minimal anti-money laundering regulation. Companies and their wholly owned subsidiaries that are publicly owned and traded on a recognised exchange generally pose a minimal money laundering risk. These companies usually have their seat in equivalent third countries with adequate, recognised regulatory schemes, and therefore pose a lower risk due to the type of business they conduct and the wider governance regime to which they are subject.
4. **Duration of the business relationship** — long-standing business relationships involving frequent customer contacts may present less risk of money laundering.
5. **Familiarity with the client's country**— including knowledge of its laws, regulations and rules, as well as the structure and extent of regulatory oversight influences risk assessment.
6. **The use of intermediate corporate vehicles** or other structures that have no apparent commercial or other rationale or that unnecessarily increase the complexity of transactions, or otherwise result in a lack of transparency, without an acceptable explanation, increases the risk.
7. **Data on persons submitted to the Office by obligated persons in the past three years** — in relation to such a person or his/her transactions there were grounds for suspicion of money laundering or terrorist financing, which increases the risk.

Equivalent third countries are countries other than the Member States of the European Union or signatories of the Agreement on the European Economic Area, which meet the same standards in the field of money laundering and terrorist financing prevention as the EU Member States. A list of equivalent third countries shall be assembled by the Inter-institutional Working Group **for** Preventing **Money Laundering and Terrorist Financing and shall be published by the Office.**

3.2.2.2 Level of customer due diligence measures

The level of due diligence must be appropriate in relation to identified risk categories. Depending on the identified money laundering or terrorist financing risk categories, and following analysis and assessment of the risk of money laundering or terrorist financing, obligated persons determine the due diligence requirements which include:

1. a standard level of due diligence to be applied to all categories to which the customer due diligence measures referred to in Article 8, paragraph (1) of the Law apply;
2. a reduced standard level of due diligence for categories in recognized low risk scenarios, where simplified customer due diligence measures apply, as prescribed by an ordinance issued by the Minister of Finance in accordance with Article 7, paragraph (5) of the Law;
3. an increased standard level of due diligence for customers identified as high risk customers, in which case enhanced customer due diligence measures apply; and

4. exemption from conducting customer due diligence measures as prescribed by Article 14, paragraph (2) of the Law or by an ordinance issued by the Minister of Finance.

Pursuant to Article 30 of the Law, obligated persons are required to apply enhanced due diligence measures in the following cases:

1. when establishing a correspondent relationship with a bank or other credit institution with a seat in a third country;
2. when establishing a business relationship with a customer that is a politically exposed person; and
3. when a customer is not physically present during the identification and identity verification procedures.

3.2.3 Low ML/TF risk

3.2.3.1 Customer Risk

A reduced standard level of due diligence can be applied to the customers referred to in Article 35, paragraph (1) of the Law, and to customers who meet the conditions determined by the Ordinance on the determination of conditions under which obligated persons identify customers as customers who pose a negligible risk in terms of money laundering or terrorist financing.

A reduced standard level of due diligence or simplified customer due diligence measures are prescribed by Article 36 of the Law.

By way of exception, when establishing a correspondent relationship with a bank or another credit institution with a seat in a third country, obligated persons have to apply enhanced customer due diligence.

3.2.3.2 Product/transaction risk

A reduced standard level of due diligence may also be applied to the following products and transactions:

1. credit agreements, where credit accounts are used exclusively for loan settlement, and loan repayment is made from an account opened in the name of a customer with a supervised credit institution;
2. transactions involving de minimis amounts for particular types of transactions (e.g. small insurance premiums, children's savings up to HRK 1,000.00 per month, deposits and withdrawals of pensions, social benefits, etc.);
3. savings deposits in housing savings banks;
4. electronic payment of certain services (e.g. the payment of parking fees or public city transportation tickets), involving de minimis amounts (HR 1,125). By way of exception, if the transaction issuer is unknown, the verification of the issuer's identity can be omitted.

3.2.4 Moderate ML/TF risk

Obligated persons shall identify as medium risk category those customers, business relationships, products or transactions that, based on the risk analysis and assessment, cannot be identified as posing a high or a low risk. In such cases, the obligated persons will act in accordance with the provisions of the Law governing the area of standard customer due diligence.

3.2.5 High ML/TF risk

3.2.5.1 Customer risk

An increased level of standard due diligence is applied where the customers are:

1. politically exposed foreign persons;
2. persons who are not physically present at the identification and identity verification during the conduct of due diligence;
3. foreign legal persons who do not, or may not, conduct trading, manufacturing or other activities in the country of registration;
4. customers, the organisational structure or nature of the legal personality of which makes it difficult or impossible to identify the beneficial owner;
5. foreign legal persons carrying out the operations referred to in Article 3, item (21) of the Law, and having unknown or hidden owners and secret investors or managers;
6. customers whose beneficial owners are subject to sanctions imposed in the interest of international peace and security in accordance with the legal acts of the EU and resolutions of the UN Security Council;
7. cash intensive business entities including:
    (a) remittance houses, authorised exchange offices, money transfer agents and other companies offering money transfer services;
    (b) casinos, betting houses and other activities related to games of chance; and
    (c) companies that, while not normally cash intensive, use substantial amounts of cash for certain transactions;
8. charity and other non-profit organisations, especially those operating on a "cross-border" basis, or those seated in a high-risk geographic area, or some of their founders or members are natural or legal persons seated or domiciled in a higher-risk geographic area;
9. accountants, lawyers, or tax advisors and others, holding accounts with a particular financial institution, and acting on behalf of their clients;
10. customers conducting their business relationships or transactions in unusual circumstances, such as:
    (a) a considerable and unexplained geographic distance between the seat of the obligated person and the location of the customer;
    (b) frequent and unexplained movements of accounts to different obligated persons;
    (c) frequent and unexplained transfer of funds among obligated persons at different geographic locations;
11. persons in relation to which the Office has, in the past three years:
    (a) requested from the obligated person to supply data due to suspicion of money laundering or terrorist financing;
    (b) ordered the obligated person to suspend the execution of a suspicious transaction; or
    (c) ordered the obligated person to monitor the customer's financial operations on an ongoing basis;
12. natural or legal person and other entities included in the list of persons subject to measures issued by the UN Security Council or by the EU — the relevant measures include financial sanctions requiring the freezing of the funds in the account and/or the prohibition of free disposal of assets, a military embargo on the arms trade with the entity, etc.;
13. natural or legal persons having their residence or seat in entities which are not subject to international law, i.e., which are not internationally recognised (due to their facilitating the fictitious registration of legal persons, issuance of fictitious identification documents, etc.);

3.2.5.2 Transaction/business relationship risk

Transactions or business relationships posing a high risk include:

1. transactions intended for persons or entities that have been subjected to measures issued by the UN Security Council or EU;
2. transactions a customer might carry out in the name and for the account of a person or an entity that has been subjected to measures issued by the UN Security Council or EU; and

3. business relationships that might be established to the benefit of a person or an entity included in the list of persons or entities that have been subjected to measures issued by the UN Security Council or EU.

3.2.5.3 Risk of a business relationship with another credit institution

The establishment of a correspondent relationship with a bank or another credit institution with a seat in a third country, other than the equivalent third country referred to in item 3.2.2.1 of these Guidelines poses a high risk.

Pursuant to Article 31 of the Law, when establishing a correspondent relationship with a bank or another credit institution with a seat in a third country, obligated persons are required to carry out the measures referred to in Article 8, paragraph (1) of the Law within the framework of enhanced customer due diligence and additionally collect the following data, information and documentation:

1. the date of issuance and validity period of authorisation to provide banking services, and the name and seat of a competent third-country authority that issued the authorisation;
2. a description of the implementation of internal procedures relating to money laundering and terrorist financing prevention and detection, particularly the procedures of customer identity verification, beneficial hidden identification, reporting to the competent bodies on suspicious transactions and customers, record keeping, internal audit and other procedures that the bank or other credit institution adopted in relation to money laundering and terrorist financing prevention and detection; a description of systemic arrangements in the field of the ML/TF prevention and detection in effect in a third country in which the bank or other credit institution has its seat or in which it has been registered;
3. a written statement confirming that the bank or other credit institution does not operate as a shell bank;
4. a written statement confirming that the bank or other credit institution neither has business relationships with shell banks established, nor does it establish business relationships or conduct transactions with shell banks;
5. a written statement confirming that the bank or other credit institution falls under the scope of legal supervision in the country of its seat or registration, and that it is required to apply legal and other regulations in the field of the ML/TF prevention and detection in accordance with that country's effective laws.

In the context of enhanced due diligence, when establishing a correspondent relationship with a bank or another credit institution having its seat in a third country, obligated persons should provide the following additional documentation:

1. a written statement that the bank or other credit institution has verified the identity of a customer and that it conducts ongoing due diligence of customers who have direct access to payable-through accounts, and
2. a written statement that the bank or other credit institution can provide, upon request, relevant data obtained on the basis of due diligence of customers having direct access to payable-through accounts.

The assessment of a credit institution's exposure to the ML/TF risk is carried out in accordance with the risk criteria and elements set out in the following risk matrix:

Low risk	Moderate risk	High risk
Stable, known customer base.	Customer base increasing due to branching, merger, or acquisition.	A large and growing customer base in a wide and diverse geographic area.
No electronic banking (e-banking), and the website is only informational, i.e. non-transactional.	The bank is beginning to introduce e-banking services and offers limited products and services.	The bank offers a wide array of e-banking products and services (i.e. account transfers, e-bill payment, or account opening

		via the Internet).
There are a few high-risk customers and businesses.	There is a moderate number of high-risk customers and businesses. The latter may include cheque cashers, convenience stores, money transmitters, exchange offices, import or export companies, offshore corporations and politically exposed persons.	There is a large number of high-risk customers and businesses. The latter may include cheque cashers, convenience stores, money transmitters, exchange offices, import or export companies, off-shore corporations and politically exposed persons.
No accounts with foreign correspondent financial institutions. The bank does not engage in pouch activities, nor does it offer special-use accounts or payable-through accounts (PTAs).	The bank has a few foreign correspondent financial institution accounts with financial institutions having adequate AML policies and procedures from low-risk countries, and minimum pouch activities, special-use accounts or PTAs.	The bank has a large number of foreign correspondent financial institution accounts with financial institutions having inadequate AML policies and procedures, particularly those located in high-risk countries, or offers substantial pouch activities, special-use accounts, or PTAs.
The bank offers limited or no private banking services or trust and asset management products or services.	The bank offers limited domestic private banking services or trust and asset management products or services over which the bank has investment discretion. A strategic plan is to increase the volume of these operations.	The bank offers a large number of domestic and international private banking or trust and asset management products or services. The private banking or trust and asset management services are on the increase. Products offered include investment management services, and trust accounts are predominantly non-discretionary, in contrast to those over which the bank has full investment discretion.
A few international accounts or a very low volume of currency activity across the accounts.	A moderate number of international accounts with unexplained currency activity.	A large number of international accounts with unexplained currency activity.
A limited number of funds transfers for customers and non-customers, limited third-party transactions, and no foreign funds transfers.	A moderate number of funds transfers; a few international funds transfers from personal or business accounts with typically low-risk countries.	A large number of funds transfers and payable-upon-proper-identification transactions; frequent transfers of funds from personal or business accounts to or from high-risk countries, offshore financial centres or financial secrecy haven countries.
No transactions with customers from high-risk geographic locations.	A minimum number of transactions with customers from high-risk geographic locations.	Significant volume of transactions with customers from high-risk geographic locations.

Low turnover of key personnel or frontline personnel (i.e. customer service representatives, tellers, or other branch personnel).	Low turnover of key personnel, but frontline personnel in branches may have changed.	High turnover, especially in key personnel positions.

The obligated person's staff member who establishes a correspondent relationship with a bank or another credit institution with a seat a third country and who performs enhanced customer due diligence is required to obtain a written approval of the superior responsible person prior to establishing the business relationship.

An obligated person is not allowed to establish or continue a correspondent relationship with a bank which operates or might operate as a shell bank or with another similar credit institution known to enter into agreements on opening and keeping accounts with shell banks. In addition, Article 31, paragraph (4), items (1), (2) and (3) of the Law shall apply.

3.2.5.4 Foreign politically exposed persons

Pursuant to Article 32 of the Law, obligated persons are required to apply an adequate procedure to determine whether or not a customer is a foreign politically exposed person. The procedure is defined by an internal bylaw, taking into account these Guidelines.

When determining whether or not a person is a politically exposed person, institutions may proceed in one of the following ways:

1. request information directly from a customer by means of a written form;
2. collect information from public sources (information that is publicly available through the media - press, TV or Internet);
3. collect information by accessing commercial data bases which include lists of politically exposed persons.

3.2.5.5 Country risk

Customers that pose a high risk may be customers having permanent residence or a seat in the following countries:

1. countries subject to sanctions, embargoes or similar measures issued by the United Nations;
2. countries identified by credible sources as:
   (a) lacking appropriate laws, regulations and other measures for the prevention of money laundering and terrorist financing;
   (b) providing funding or support for terrorist activities and having designated terrorist organisations which operate within them;
   (c) having significant levels of corruption, or other criminal activity;
3. countries which are not Member States of the European Union or signatories to the Treaty Establishing the European Economic Area, and do not qualify as equivalent third countries;
4. countries which, according to the FATF data, belong to non-cooperative countries or territories or, in the case of an Offshore Financial Centre from the list supplied by the Office.

As regards information on high-risk countries or non-cooperative countries or territories that do not meet key international standards for the ML/TF prevention, you are advised to visit the official web sites of the following international bodies:
MONEYVAL[5], www.coe.int/t/dghl/monitoring/moneyval, and FATF[6], www.fatf-gafi.org.

[5] MONEYVAL is a regional body within the Council of Europe, established in 1997, which consists of the members of the Council (including the RC); its objective is to assess the status of the fight against money

3.2.5.6 Product risk

The increased level of standard verification should be applied to the following products or services:

1. services identified by competent authorities or other credible sources as potentially posing an enhanced risk, for example, establishing correspondent relationships with credit institutions having their seats in third countries;
2. services involving banknote and precious metal trading and delivery;
3. services that provide more anonymity or that can be readily provided across international borders, such as online banking, stored value cards, international wire transfers, the services of private investment companies and trusts, non-government organisations, etc.

3.2.5.7 Enhanced customer due diligence measures

Articles 31, 32 and 33 of the Law prescribe enhanced customer due diligence that obligated persons are required to perform when establishing correspondent relationships with third-country credit institutions, or business relationships with politically exposed persons, as well as in the cases of customer absence.

With respect to other customers, business relationships and transactions identified as posing a high risk, obligated persons should, within the framework of increased level of standard verification, implement appropriate measures and controls aimed at reducing the exposure to identified ML risks. These measures and controls may include:

1. the monitoring of all areas of customers' operation, their business relationships, products and high risk transactions;
2. an increased level of determination and verification of customer identity;
3. imposing stricter requirements for approvals to open accounts or establish business relationships;
4. closer transaction monitoring; and
5. increased levels of ongoing controls and frequency of business relationship reviews.

The same measures and controls may address more than one of the risk criteria identified, and obligated persons are not necessarily expected to introduce specific controls with respect to each of the risk criteria.

3.2.6 New technologies providing for anonymity

Pursuant to Article 34 of the Law, obligated persons are required to pay special attention to any ML/TF risk which may stem from new technologies enabling anonymity and to put in place policies and take measures aimed at preventing the use of such new technologies for ML/TF purposes.

Obligated persons must put in place policies and procedures for the risk involved in business relationships or transactions with customers who are not physically present, and apply them when establishing a business relationship with a customer, and during the performance of the customer due diligence, while taking into account the provisions of Article 33 of the Law, governing the procedures to be followed by an obligated person when establishing a business relationship without the presence of the customer.

---

laundering and terrorist financing in the Council of Europe member countries. The assessment is based on the FATF and EU standards, as well as conventions of the Council of Europe and UN.

[6] FATF (Financial Action Task Force) is an international body, established in 1989, which has developed 40 recommendations outlining measures for the prevention of money laundering and terrorist financing, recognised as a standard for fighting money laundering and terrorist financing,

In the process of defining the said policies and procedures for the risk involved in business relationships or transactions with customers who are not physically present, or in the process of defining policies and applying measures for the prevention of the use of new technologies for ML/TF purposes, obligated persons are recommended to apply the obligations, principles and rights governed by the Credit Institutions Act (Official Gazette 117/2008, 74/2009 and 153/2009) and the bylaws pertaining thereto, notably the Decision on Adequate Information System Management (Official Gazette 37/2010.) and Guidelines for Information System Management Aimed at Reducing Operational Risk.

3.3 Customer due diligence measures

Pursuant to Article 8 of the Law, obligated persons are required to carry out the following customer due diligence measures:

1. identifying the customer and verifying the customer's identity on the basis of documents, data or information obtained from a credible, reliable and independent source;
2. identifying the beneficial owner of the customer and verifying the beneficial owner's identity;
3. collecting data on the purpose and intended nature of a business relationship or transaction and other data in accordance with the Law; and
4. ongoing monitoring of the business relationship, including close scrutiny of transactions carried out during that relationship, in order to ensure that these transactions are consistent with the obligated person's knowledge of the customer, the type of his/her business and risk, including, where necessary, information on the source of funds; the documents and data available to the obligated person must be up-to-date.

Obligated persons which are unable to carry out the customer due diligence measures referred to in Article 8, paragraph (1), items (1), (2) and (3) of the Law, may not establish a business relationship or carry out a transaction, or must terminate an existing business relationship and send a notification thereof to the Office, accompanied by all previously collected data on the customer or transaction, in accordance with Article 42 of the Law.

3.3.1 Obligation to identify a customer and verify the customer's identity; exemptions

Pursuant to Article 9 of the Law, obligated persons must 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 other contractual relationship established or concluded by a customer with an obligated person, which is of a relatively long duration, which enables ongoing monitoring;
2. when carrying out a transaction amounting to HRK 105,000.00 or more, whether the transaction is a single one or it includes several interrelated transactions totalling HRK 105,000.00 or more. In contrast to a business relationship, in the case of a transaction the emphasis is on a one-off nature of the activity.
3. when there are doubts about the credibility and veracity of the previously obtained information on a customer or the customer's beneficial owner;
4. in all instances when there are grounds for suspicion of ML/TF in relation to a transaction or a customer, regardless of the transaction value.

Exemptions from the obligation to carry out due diligence measures for certain products

Electronic money institutions, electronic money institutions from another Member State and branches of third-country electronic money institutions may be exempted from the obligation to carry out customer due diligence measures in the following cases:

1. when issuing electronic money, if a single amount of a payment executed for the issuance of such money, on an electronic data carrier which may not be recharged, does not exceed the kuna equivalent of EUR 150.00;

2. when issuing electronic money and dealing with electronic money, if the total amount of executed payments, stored on an electronic data carrier which may be recharged, does not exceed the kuna equivalent of EUR 2,500.00 during a calendar year, except in the cases where the electronic money holder cashes the kuna equivalent of EUR 1,000.00 or more during the same calendar year.

Obligated persons may be exempted from the obligation to carry out the customer due diligence measures in the case of other products or transactions associated with them, which pose negligible ML/TF risks, provided they meet the conditions prescribed by an ordinance of the Minister of Finance.

By way of exception, obligated persons may not be exempted from the obligation to carry out customer due diligence measures when there are grounds for suspicion of ML/TF with respect to a customer, product or transaction.

Bearing in mind the activity of electronic money institutions - mobile network operators which, in addition to their primary activity, provide the services of executing payment transactions where the consent of the payer to execute a payment transaction is given by means of a telecommunication, digital or IT device and the payment is made to a telecommunication, a network or an IT system operator, acting exclusively as an intermediary between the payment service user and the supplier of goods and services, electronic money means only that part of the stored monetary value which has been used for the payment of certain goods and services.

The amounts paid by prepaid users to their accounts for the purpose of recharging them where these accounts are used for telecommunication services provided by a mobile network operator, are not considered as electronic money. The measures and actions against ML/TF are only applied in the part relating to payment services connected with electronic money.

3.3.2 Identification of the beneficial owner

Obligated persons are required to identify a customer's beneficial owner in accordance with Article 23 of the Law.

3.3.2.1 Identification of the beneficial owners of associations, endowments, foundations, political parties and religious communities

1. Where the customer is a non-profit organisation, such as an association, attention should be focused on activities through which the statutory goals are achieved, reasonable measures should be taken to identify the founder, and the identity of one and/or more persons controlling or managing the customer's activities, including the members of the governing and representative bodies, should be established.

These data are obtained from publicly available registers (a register of associations) or directly from the non-profit organisations concerned. Given that associations do not have capital divided into shares or stakes, the customer is not required to provide data on the natural person directly or indirectly holding more than 25% of shares, stakes or votes in the legal person.

2. Where the customer is a non-profit organisation which administers and distributes monies, such as an endowment or a foundation, or where it conducts legal transactions, such as trust dealings, the

beneficial owner is a legal person holding 25% or more of the property rights of a particular legal transaction, if future beneficial owners have already been identified.

Where future beneficial owners have not yet been identified, the beneficial owner shall be the person in whose main interest the legal transaction is conducted, i.e. in whose main interest the business is done, or in whose main interest the legal person has been established. A natural person who controls 25% or more of the property rights of a particular legal transaction is considered to be the beneficial owner.

The data necessary to identify the beneficial owner are obtained directly from the customer or from publicly available registers. Obligated persons obtain data from an endowment or foundation administrator, or from a trustee who manages certain property, relating to one or more natural and/or legal persons who have established the endowment or the foundation, or relating to persons on whose behalf the trustee decides on the property management. The registers (endowment book, foundation book, etc.) are public registers offering free access to every interested party that can request excerpts from such registers or copies of documents from a file (articles of association, a statute, a decision approving the establishment of an endowment or other documents on the basis of which an entry in the book or a change in the data has been made.

3. Political parties, trade unions and religious communities do not have beneficial owners**.**

4. Where the customer is an embassy, obligated persons conduct the simplified customer due diligence referred to in Article 35 of the Law, which excludes the identification of the beneficial owner.

3.3.2.2 A natural person exercising control over a legal person's management board without ownership of shares/stakes

Pursuant to Article 23, item (1), second indent of the Law, in the case of legal persons, branches, representative offices and other entities subject to domestic and foreign law and equated to a legal person, the beneficial owner shall be a natural person who otherwise exercises control over the legal person.

This provision applies, for example, to limited liability companies, whose articles of incorporation provide that the company's management board is appointed by an individual company member. According to the Companies Act, members of a limited liability company's management board are appointed by the company's assembly, but, subject to the articles of incorporation, this right may be transferred to somebody else, e.g. the supervisory board, one of the company's bodies or even a company member. Hence, a natural person who is a company member determined by the articles of incorporation as a person to appoint the members of the management board, can be considered as the beneficial owner in terms of Article 23, item (1), second indent of the Law.

3.3.3 Identification and identity verification of a customer who is not physically present

Pursuant to Article 33 of the Law, if the customer is not physically present during the identification and identity verification, the obligated person shall be required to apply the following enhanced customer due diligence measures:

1. collect additional documents, data or information on the basis of which the customer's identity is to be verified;
2. additionally verify the submitted documents or additionally certify them by the foreign credit or financial institution referred to in Article 3, items (12) and (13) of the Law;
3. apply a measure whereby the first payment within the business activity is made through an account opened in the customer’s name with another credit institution.

The additional documents, data or information on the basis of which the customer's identity is verified may include the following:

1. for residents, proof of permanent residence obtained from the competent authority that keeps civil status records, or certificate of permanent residence issued by the competent Police Department; for non residents, proof obtained from, e.g. a credit reference agency;
2. personal references (e.g. from an existing obligated person's customer);
3. previous bank references and bank contacts with respect to the customer;
4. data on the source of funds and assets which are or will be the subject of the business relationship;
5. a certificate of employment or of a public office held by the person.

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

1. by verifying the date of birth on the basis of an official document (e.g. a birth certificate, a passport, an ID card or social security records);
2. by verifying the permanent address (e.g. through utility bills, tax apportionment, bank statements or letters from public authorities);
3. by contacting the client by telephone, letter or e-mail for the purpose of verifying the supplied information after the account has been opened (e.g. a disconnected telephone line, a returned letter or an inaccurate e-mail address should indicate a need for further checks); or
4. by checking the validity of official documentation by means of a certificate issued by an authorised person (e.g. an embassy officer or a public notary).

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

1. by examining the copies of the latest business report and financial statements (audited, if available);
2. through an examination carried out by the Business Information Centre or on the basis of a statement given by a reputable and well-known attorney or an accounting company that verifies the submitted documents;
3. by examining the company or carrying out some other type of review in order to verify that the company has not ceased operating, or been removed from the register or liquidated, or that it is not in the process of terminating its operation, removal from the register or liquidation;
4. by an independent verification of information, e.g. through an access to public and private data bases;
5. by obtaining prior references of the obligated person; and
6. by contacting the company via telephone, mail or e-mail.

In some jurisdictions, there may be other equivalent documents to provide satisfactory proof of a customer's identity.

3.3.4. Data on the payer in the case of electronic funds transfer

The main determinants of electronic funds transfer, i.e. of the obligation to collect data on the payer and the procedure to be followed by payment service providers are specified in Article 15 of the Law.

Pursuant to Article 15 of the Law, the Minister of Finance has issued an Ordinance on the content and type of data on the payer, accompanying the electronic funds transfer, on the obligations of payment service providers and on exemptions from the obligation to collect data for the purpose of transferring funds.

The payee's payment service provided is required to:

1. collect accurate and complete data on the payer and include them in a form or a message accompanying the electronic transfer of funds, sent or received in any currency. The data must accompany the transfer at all times throughout the chain of payments;
2. refuse a funds transfer which contains incomplete data on the payer, i.e.: the payer's name and surname, address and account number;
3. have in place effective procedures to establish whether the data on the payer are complete and to check whether the payer data fields within a payment and settlement system used for transferring funds are filled in with letters or characters allowed by that payment and settlement system's conventions.

Should the data on the payer's account number not be available, it can be replaced by the unique reference number, and the payer's address can be replaced by the personal ID number (OIB) or national identification number of the payer. The payee's payment service provider shall consider the lack of data on the payer, with respect to the assessed risk level, as a potential reason to apply the enhanced customer due diligence measures.

3.3.5 Entrusting a third party with the conduct of customer due diligence

When establishing a business relationship with a customer, obligated persons may, under the conditions lad down by the Law and subordinate legislation, entrust a third party with the conduct of the identification and identity verification procedures.

Obligated persons must check upfront whether the third party they are about to entrust with the conduct of customer due diligence meets all the conditions prescribed by the Law.

The customer due diligence conducted for an obligated person by a third party may not be accepted if the third party conducted the identification and identity verification procedures without the presence of the customer.

3.4 Monitoring a customer's business activities and notifying the Office

3.4.1 Business relationship monitoring measures

Obligated persons must closely monitor transactions carried out during the business relationship, in order to ensure that the transactions are consistent with the obligated person’s knowledge of the customer, type of business, source of funds and the purpose and intended nature of the business relationship or a transaction. They are required to ensure that the volume and frequency of the business relationship monitoring measures are in line with the ML/TF risk to which they are exposed in running a business or dealing with a customer, pursuant to Article 7 of the Law.

Obligated persons are required to conduct a repeated annual due diligence of a foreign legal person, regularly once a year, but no later than after the expiry of one year since the last customer due diligence has been conducted.

The annual customer due diligence is also obligatory for a customer which is a legal person with a seat in the RC, conducting transactions in the amount of HRK 105,000.00 or more, and which is 25% or more owned by:
1. a foreign legal person which does not or may not engage in trading, manufacturing or other activities in the country of registration; or
2. a fiduciary or another similar company subject to foreign law, having unknown or hidden owners and secret investors or managers;

3.4.2 Notifying transactions to the Office

3.4.2.1 Obligation to notify the Office of cash transactions and notification deadlines

Obligated persons are required to notify the Office immediately of each cash transaction in the amount of HRK 200,000 or more, but no later than three days from the date of execution of such a transaction. The cash transaction notification form comprises the data prescribed by the Ordinance on the obligation to report cash transactions in the amount of HRK 200,000.00 or more to the Anti-Money Laundering Office, and on conditions under which obligated persons are not required to report cash transactions of certain customers to the Anti-Money Laundering Office.

3.4.2.2 Obligation to notify the Office of suspicious transactions and persons and notification deadlines

Obligated persons are required to notify the Office immediately of a suspicious transaction prior to its execution, and to indicate, among other things, the grounds for suspicion of ML/TF. By way of exception, where an obligated person has been unable to notify the Office in the prescribed manner of a suspicious transaction prior to its execution, due to the nature of the transaction, or the fact that the transaction had not been executed, or for other justified reasons, the obligated person is required to notify the Office subsequently, but no later than the next business day. The suspicious transaction report must be accompanied by documents to substantiate the reasons for not acting in the prescribed manner.
The Office should be notified of suspicious transactions prior to their execution by telephone, fax or in another adequate manner, and after their execution in the manner prescribed by the Ordinance on the notification of the Anti-Money Laundering Office of suspicious transactions and persons.

Obligated persons are required to refrain from executing transactions which they know or suspect to be related to ML/TF. Obligated persons are required to notify the Office, immediately and in the prescribed manner, of such transactions prior to their execution, to explain the grounds for suspicion of ML/TF, which clearly indicate that a transaction or person is suspicious, and to specify indicators on the basis of which such an assessment has been made.

When establishing the grounds for suspicion of ML/TF, obligated persons are required to use the list of indicators for the detection of suspicious transactions and persons. The assessment that a transaction or person is suspicious is based on the criteria specified in the list of indicators for the detection of suspicious transactions and persons. Obligated persons are required to amend the list of indicators and adapt it to the money laundering trends and typologies known to them, as well as to the circumstances stemming from the obligated person's operation.

Where a transaction or person complies with one of the indicators, this does not necessarily mean that the transaction or person is suspicious. However, it points to a need for additional analysis prescribed in Article 43 of the Law. A broader view should be taken, being aware that obligated persons best know their clients and ensuring that the measure of ongoing monitoring of the business relationship is carried out, which includes a close scrutiny of transactions executed during that business relationship in order that these transactions are consistent with the obligated person's knowledge of the purpose and intended use of the transaction, the knowledge of the customer and of the type of business relationship and risk, including the source of funds. Should the obligated person assess, based on the analysis made, that there are grounds for suspicion that a transaction or person is related to money laundering, the obligated person is required to notify the Office in a prescribed manner of such a transaction prior to its execution.

3.4.2.3 Complex and unusual transactions

Obligated persons must pay special attention to complex and unusually large transactions, as well as to each form of transaction having no apparent economic or visible lawful purpose, even if grounds for suspicion of ML/TF with respect to such a transaction have not yet been established.

In addition, obligated persons must analyse the background and purpose of such transactions and make a written record of the analysis results, in order to make them available at the request of the Office or another supervisory body. The purpose of the report on the analysis results is to explain the reasons for not reporting a particular transaction as suspicious.

An analysis of complex and unusual transactions should cover the data on:

1. the intended nature and purpose of a business relationship;
2. the customer's activities;
3. funds kept on transaction accounts;
4. the purpose and intended use of a transaction;
5. cash transaction inflow and outflow;
6. transactions with countries from enhanced-risk geographic areas;
7. persons authorised to use the accounts;
8. frequency of transactions involving a certain legal or natural person as the transaction issuer;
9. the source of funds;
10. information obtained from the media; and
11. information obtained from publicly accessible databases, etc.

Should the analysis demonstrate that there are grounds for suspicion of ML/TF, the Office should be notified accordingly. The report on a suspicious transaction or person should comprise all data obtained during the analysis, as well as the data prescribed by Article 42 of the Law.

4 AML/TF measures in business units and companies in majority ownership, having their seat in a third country

Pursuant to Article 5 of the Law, obligated persons are required to ensure that the ML/TF prevention and detection measures are applied to the same extent in their business units and in companies in which they have a majority holding or a majority of the voting rights, and which have their seat in a third country, unless this is expressly contrary to the third country's legislation.

For this purpose, business units and companies in which the obligated person has a majority holding or a majority of voting rights should be regularly informed of the obligated person's internal procedures relating to the ML/TF prevention and detection, particularly as concerns customer due diligence, data supply, record keeping, internal controls, etc.

Where the legislation of a third country does not permit the application of the ML/TF measures to the extent prescribed by the Law, the obligated person is required to notify the Office thereof and to introduce the appropriate measures for eliminating the ML/TF risk.

5 Final provisions

On the date of adoption of these Guidelines, the Guidelines for the analysis and assessment of money laundering and terrorist financing risks for credit institutions and credit unions of 9 July 2009, Dec. No: 636-020/07-09/ŽR, shall cease to have effect.

Dec. No: 138-020/06-12/ŽR

Zagreb, 18 June 2012

ANNEX XXVIII Financial Inspectorate: Guidelines for reporting entities subject to control by the Financial Inspectorate in relation to the enforcement of the Anti-Money Laundering and Terrorist Financing Act

1. Introduction

These Guidelines for the enforcement of the Anti-Money Laundering and Terrorist Financing Act (AMLTFA) (Official Gazette, 87/2008) are issued by the Financial Inspectorate of the Ministry of Finance (hereinafter: Financial Inspectorate) for the benefit of the reporting entities subject to control by the Financial Inspectorate. The Financial Inspectorate, pursuant to Article 83 of the AMLTFA (hereinafter: the Act) is responsible for the enforcement of the Act and of other bylaws passed on the basis of this Act.

These Guidelines are issued pursuant to Article 88 of the Act for the purpose of ensuring a uniform application by reporting entities subject to control by the Financial Inspectorate of the provisions of the Act and its regulations.

1.1 General

The purpose of combating money laundering and terrorist financing (ML/TF) is to prevent and detect activities used to conceal the true source of money or other property suspected to have been obtained illegally. The international community and the government recognize the vulnerability of financial and non-financial sectors to ML/TF. To this end the Act has created certain obligations, and conveyed certain rights, to the legal and natural persons operating in these specific sectors in the fight against ML/TF. Those subject to the Act are referred to as reporting entities.

Combating ML/TF requires all reporting entities to effectively implement the measures outlined in these guidelines to minimize the risk that people called "launderers" and "terrorist financiers" find the weakest link or use new channels for misuse of the financial system.

All sectors identified as reporting entities run the risk of being misused for ML/TF purposes. These sectors have been identified by the international community through the Financial Action Task Force (FATF) as more vulnerable than others and as such Croatia joins a global effort to combat money laundering and terrorist financing. While all sectors identified in the legislation and in these guidelines face common challenges in identifying, mitigating and monitoring ML/TF risks, many sectors face specific risks. These guidelines provide both common and specific risks and indicators in identifying ML/TF. Various sectors, in addition, face specific vulnerabilities and challenges and for this purpose these guidelines include references to specific sector challenges.

Money laundering and terrorist financing involve actions that represent a threat to the stability and integrity of the financial system which in the long term weakens citizens' confidence in the democratic principles of a modern society, on both global and national levels, and leads to the increased necessity for supervising and monitoring of the financial system for the purpose of preventing and detecting activities linked with ML/TF.

1.2 Purpose of the guidelines

Awareness of obligations is a critical component for the prevention of ML/TF by reporting entities. These guidelines are issued for the purpose of assisting reporting entities in meeting their obligations and facilitating their implementation of the required legislative and regulatory measures to prevent the misuse of the financial system for money laundering and terrorist financing purposes in the Republic of Croatia. As part of their obligations under this Act and its regulations, all reporting entities are required to implement measures listed in the Act including four broad categories of requirements described in section 3 of these Guidelines.

Reporting entities are also obliged to align the procedures described in this Guideline with valid guidelines passed by competent supervisory bodies.

1.3 The Financial Inspectorate

The Financial Inspectorate is a Directorate of the Department of Finance responsible for the administration and enforcement of the Anti-Money Laundering and Terrorist Financing Act (the Act) which came into force on January 1, 2009. It is empowered and guided in its administration by the Financial Inspectorate of the Republic of Croatia Act and other national laws.

Its workforce of approximately 50 employees staff contribute to combating money laundering and terrorist financing in the Republic of Croatia.

In achieving its mission to assist in protecting Croatia from the serious consequences of money laundering and terrorist financing to the economic, social, security and political interests of the country, the Financial Inspectorate carries out a number of functions including ensuring compliance with anti-money laundering and anti-terrorism obligations by reporting entities, cooperation with other government agencies, issuing recommendations for the uniform application of provisions of the Act, participating in the advanced training of employees of reporting entities, administering misdemeanor proceedings and providing assistance in investigations and court proceedings.

Working in partnership

The Financial Inspectorate cannot work alone in combating money laundering and terrorist financing. It works in partnership with reporting entities, representatives of professional bodies, sector representatives, other government bodies and international partners. In conjunction with other supervisory bodies, the Financial Inspectorate assists reporting entities in understanding the application of the Act and in verifying compliance.

Reporting entities play a crucial front-line role in preventing and detecting money laundering and terrorist financing. It is through the compliance efforts of reporting entities, refusing to process suspicious transactions, keeping records and reporting to the Anti-Money Laundering Office that reporting entities play a pivotal role in the national anti-money laundering and anti-terrorist financing regime. Therefore it is critical for reporting entities to understand the law they must apply, their obligations, the role of the Financial Inspectorate and the procedures they need to implement. It is in this spirit of partnership that the Financial Inspectorate will conduct its activities and relations with reporting entities in a manner that will reflect the following values:

- **Fair treatment**: legislative measures will be applied fairly and impartially.
- **Courtesy and consideration**: reporting entities will be treated with courtesy, respect and consideration.
- **Privacy and confidentiality**: personal, transactional and financial information will be protected against unauthorized use or disclosure.
- **Information**: reporting entities will be entitled to complete, accurate and clear information about their obligations.

With these guidelines, we hope that reporting entities be better informed to fulfil their obligations and that as the Financial Inspectorate we will be able to rely more effectively on the support of reporting entities to combat money laundering and terrorist financing.

1.4 Money Laundering

The objective of this section is to provide reporting entities with a basic understanding of money-laundering by defining it, describing it as a three-phased process and providing a brief synopsis of some of the most commonly used money-laundering methods.

1.4.1 Definition of money laundering

According to the Act, money laundering is defined as: " …the undertaking of actions aimed at concealing the true source of money or other property or right suspected to have been obtained in an illegally in the country or abroad, including:

- Conversion or any other transfer of money or other property derived from criminal activity;
- The concealment of the true nature, source, location, disposition, ownership or rights with respect to money or other property derived from criminal activity; and
- The acquisition, possession or use of money or other property derived from criminal activity."

A criminal activity always precedes the money laundering offence, that is, the concealment of the true source of the proceeds of crime and all property derived from those proceeds.

1.4.2 Money laundering phases

The process of laundering money is described in three phases:

- **Placement:** funds derived from criminal activities (for example, drug trade) are introduced (placed) for the first time in the financial system or are used to buy high-value goods or property. In this phase, the so-called "dirty money" is most visible and exposed to detection.

- **Layering:** in this phase, funds are layered and placed in financial flows. Performing complex transactions is an attempt to conceal, in various ways, the source of illegally acquired funds or the owner of the funds. In this phase, the detection of "dirty money" becomes more complicated.

- **Integration**: in this phase the dirty-money reaches its goal when it is integrated into the financial system as part of the flow of legitimate funds, attaching itself to other financial instruments or values within the country's financial system thus making detection nearly impossible.

1.4.3 Money laundering methods

Alongside technological developments, there is also an increase in the number of sophisticated and complex methods used for the purpose of concealing the origin of illegally acquired property. Out of a great number of methods, the following are some of the most often used by "launderers" attempting to circumvent detection:

Multiple transactions – if the same person in one day performs two or more transactions, and the total addition of transactions in one day exceeds the prescribed limit for identification or reporting to the Anti-Money Laundering Office (hereinafter: Office).

False companies – so-called "shell companies" conceal the laundered funds while "front companies" perform legal business activities in order to conceal the money laundering. This method is often used in the layering phase while the money laundering procedure itself can be conducted in several countries.

Casinos – a person purchases casino tokens with cash, plays several series with a few tokens and asks for a pay-out of the majority of the remaining tokens which he/she deposits later in the account of third persons.

Use of a nominee – this is the most often used method for laundering money at the placement phase. A person who wishes to introduce dirty money into the financial system may attempt to conceal the origin of illegally acquired property by engaging "nominees" such as family members, friends or business associates who enjoy the confidence of the community and perform transactions on his/her behalf. In this way the nominee may more easily avoid detection of the source of the dirty money by reporting entities.

Structuring – "smurfing" is term synonymous with the smallish animated cartoon characters. Smurfing involves structuring larger amounts of cash, above the legislated threshold for record keeping and reporting, into smaller cash transaction amount for placement into the financial system. The launderer may use many "smurfs" to structure his dirty money. By structuring the larger cash deposit into smaller deposits, often deposited by many "smurfs", the launderer is attempting to avoid several detection methods created as part of the ML/TF regime such as: the obligation of reporting on cash transactions over a certain amount (€15,000) and the obligation of identifying the client. For these reasons, "smurfs" are often in the ML/TF process.

Purchasing of property with cash - when buying high-value goods or luxury products (jewels, vehicles, yachts and the like) as well as real estate and land using cash, most often the property is registered in the name of a close associate or a relative for the purpose of concealing the beneficial owner. The property is also often resold in order to conceal its true origin and its beneficial owner.

Currency repurchase – illegally acquired funds are used for buying foreign currency which is then most often transferred to bank accounts in offshore financial centres around the world.

Refining - smaller denominations (€ 10 or €20) of illegally acquired funds, such a funds acquired through street level drug dealing, are changed for larger denominations (€100, €200 or €500) for concealment purposes on cross-border movements.

Reporting entities should refer to various sources and maintain their knowledge of money laundering trends and typologies by consulting the Annexes included in these Guidelines as well as information and guidance provided by Financial Intelligence Unit, the Financial Action Task Force and other international bodies. Annexes 1, 2 and 3 include general, sector specific ML/TF indicators and high risk indicators respectively.

1.4.4 The importance of combating money laundering

Criminals engage in illegal activities for the purpose of acquiring funds. Once gained, the "dirty money" needs to be "laundered" so that it can be legally used. "Laundered" or legalized funds provide a legitimate basis to criminal groups for further accumulation of wealth and consequently for leading and expanding a criminal empire.

Economic and political influence of criminal organizations weakens social values, ethical standards and, finally, institutions of a modern democratic society. In addition, money laundering has a negative impact on economic indicators and contributes to the weakening of economic growth.

Globalization is a process which gradually abolishes restrictions in the flow of goods, services, people and capital among different countries and parts of the world, and this makes people anywhere in the world more exposed to dangers of the heaviest forms of financial crime. Combating money laundering is a very complex and challenging undertaking in our modern time requiring national and international cooperation throughout the enforcement process: awareness, detection, investigation, seizure of assets, prosecution and confiscation/recovery of funds.

1.5 Financing of terrorism

1.5.1. Definition

Terrorism, in its broadest sense, implies any use of violence for the purpose of achieving political goals. Violence is a means of compulsion over certain subjects (state, international organization etc.) in order to do something or to fail to do something. There are various underlying objectives to terrorism. They include the achievement of political, ethnic and religious objectives. According to the provision of the EU Council Framework Decision on combating terrorism, from June 13th 2002, a terrorist act is: "… an act which, considering its nature and context, may seriously damage a country or an international organization and which is committed with an intention of seriously deterring people or illegally forcing a government to do something or to refrain from doing it or serious destabilizing or destruction of fundamental political, constitutional or economic structure of a country or international organization." The provisions of the Criminal Code of the Republic of Croatia referring to terrorism fully comply with the mentioned Framework Decision.

Terrorist financing represents a problem which, in today's time, seriously preoccupies the whole international community. The intensity of international terrorist activities depends on the funds that terrorists can collect, so it is extremely important to uncover and disable in a timely manner any attempt to finance terrorist activities.

1.5.2. Methods used for terrorist financing

There are two primary methods of financing terrorist activities. The first method involves the collection of financial aid from countries, organizations or individuals, while the second one involves activities generating a profit but which can be both legal and illegal.

a. Collection of financial aid

Members of terrorist groups can be financed for their terrorist activity by a government of some country or organizations, but lately this financing method is in decline. The support of a country is replaced by a support from other sources like individuals owning significant financial funds or pooled funds from unsuspecting donors to non-profit organizations.

b. Activities generating proceeds of crime

Sources of terrorist financing may be legal or illegal, may come from criminal activities like fraud, drug trade or kidnapping, but they also may come from legal sources like loans, membership fees, selling of publications, donations etc. Kidnappings and extortions have a double goal, to financially support a terrorist organization while at the same time spreading concern and fear in a target population or a group of people.

1.5.3. Connection between money laundering and terrorist financing

Methods used by terrorist groups for generating/collecting financial funds from illegal sources are similar to methods used by other criminal organizations. Like other criminal groups, they also have to find the way to launder illegal funds in order to be able to use them without attracting the attention of competent authorities.

Sources of terrorist financing may be legal or illegal, may come from criminal activities like fraud, drug trade or kidnapping, but they also may come from legal sources like loans, membership fees, selling of publications, donations, etc. Terrorism financing does not always include great amounts of money; transactions do not necessarily have to be complex as it is the case with money laundering. However, methods used by terrorist organizations for transferring, collecting and concealing sources of financing remain similar to those used by criminal organizations for money laundering purposes. Therefore, a comprehensive and effective regime of preventing money laundering is a key for monitoring financial activities of terrorist groups.

1.5.4. The importance of combating terrorist financing

According to Article 2 of the 1999 International Convention for the Suppression of the Financing of Terrorism, an offence of financing terrorism is committed by any person who, by any means, directly or indirectly, unlawfully and wilfully, provides or collects funds with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out an act which constitutes an offence within the scope of and as defined in the existing antiterrorist conventions of the United Nations, or any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act.

The duty of a country to implement measures for the prevention of financing of terrorism was also established by the United Nations Security Council Resolution 1373 from 2001, by which the Security Council's Counter Terrorism Committee was founded, having the responsibility to monitor the member states' compliance with the provisions of this Resolution.

Terrorists or terrorist groups' activities represent a real threat to the safety and security people and society, at both local and international levels. The Republic of Croatia, on bilateral and multilateral levels within the framework of international treaties on the prevention and detection of the most serious forms of crime, specifically terrorist financing, cooperates with other countries in combating terrorism. Establishing business relationships with terrorist groups represents, for financial institutions, as well as for those performing so-called professional activities, a high reputational and operation risk resulting in severe legal consequences.

To effectively combat terrorist financing, reporting entities should refer to various sources and maintain their knowledge of money laundering trends and typologies by consulting the Annexes included in these Guidelines as well as information and guidance provided by Financial Intelligence Unit, the Financial Action Task Force and other international bodies.

2 Applicable legislation in the field of money laundering and terrorist financing prevention

2.1 Linkage between the Anti-Money Laundering and Terrorist Financing Act and ordinances passed on the basis of this Act

The Anti-Money Laundering and Terrorist Financing Act is in line with international standards set by the Financial Action Task Force and the Guidelines of the European Parliament and the Council 2005/60/EC on the prevention of using the financial system for the purpose of money laundering and financing of terrorism, from October 2005 (Third Directive).

Pursuant to a legal authorization, the Minister of Finance has issued the following ordinances:

1. Ordinance on the obligation to report suspicious transactions and persons to the Office for Money Laundering Prevention ("Official Gazette", 01/09)

2. Ordinance on the obligation to report cash transactions of HRK 200,000.00 or above to the Office for Money Laundering Prevention and on the conditions under which the reporting entities are not obliged to report cash transactions of individual clients to the Office for Money Laundering Prevention ("Official Gazette" 01/09)

3. Ordinance on the control of domestic or foreign currency cash taken in and out of the country across the state borders ("Official Gazette" 01/09)

4. Ordinance on the manner and the time limits for reporting suspicious transactions and persons to the Office for Money Laundering Prevention and on the keeping of records by attorneys at law, attorneys-at-law offices, public notaries, audit firms and independent auditors and legal and natural persons engaged in accounting and tax counselling activities ("Official Gazette" 01/09)

5. Ordinance on the content and type of data on the payer accompanying the electronic transfer of funds, on the obligations of payment services providers and on exemptions from the obligation to collect data in funds transfer ("Official Gazette" 01/09)

6. Ordinance on the determination of the conditions under which reporting entities have to identify clients as clients representing a negligible risk in terms of money laundering or financing of terrorism ("Official Gazette" 76/09)

7. Ordinance on the conditions under which persons subject to the Anti-Money Laundering and Terrorist Financing Act may outsource measures of client due diligence to third persons ("Official Gazette" 76/09)

8. The Ordinance on the manner and the time limits for submitting data on criminal activities of money laundering and terrorist financing to the Office for Money Laundering Prevention ("Official Gazette" 76/09)

9. The Ordinance on the manner and the time limits for submitting data on misdemeanour proceedings to the Office for Money Laundering Prevention ("Official Gazette" 76/09).

2.2 Criminalization of money laundering and terrorist financing activities

The money laundering offence is criminalized by Article 279 of the Criminal Code ("Official Gazette" 110/97, 27/98, 129/00, 51/01, 111/03, 190/03, 105/04, 84/05, 71/06, 110/07, 152/08) prescribing that a money laundering offence is committed by a person who, within the banking, financial or other business sector, invests, takes over, transfers, replaces, transforms or in any other way conceals the true source of money, objects, rights or property benefit for which it is known that it has arisen by virtue of or has been obtained by a criminal act.

The financing of terrorism is criminalized by a special offence of preparing criminal acts against values protected by the international law from Article 187.a of the Criminal Code in accordance with which a person shall be sentenced to prison from one to five years if he/she has given or collected funds intended to be used for committing a criminal act of terrorism from Article 169, a criminal act of public encouragement to terrorism from Article 169.a or a criminal act of recruiting and training for terrorism from Article 169.b of the Criminal Code.

2.3 International documents in the field of detection and prevention of money laundering and terrorist financing

In July 2008, The Republic of Croatia ratified the Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on financing of terrorism. The mentioned Convention is the first international instrument covering the prevention and control over the money laundering and financing of terrorism. By signing and ratifying this Convention, the Republic of Croatia has come near the end of the procedure of ratification of three pillars of legislative "arsenal" of the Council of Europe in combating terrorism (until now, the Republic of Croatia has also ratified the Additional Protocol along with the Convention on the Suppression of Terrorism in 2005 and the Convention on the Prevention of Terrorism in January 2008).

2.4 The Anti-Money Laundering and Terrorist Financing Act

The Act is in line with the Guidelines of the European Parliament and the Council 2005/60/EC on the prevention of using the financial system for the purpose of money laundering and financing of terrorism from October 2005 (Third Directive).

The Anti-Money Laundering and Terrorist Financing Act creates a level playing field for all reporting entities regarding the implementation of measures for the prevention of money laundering and financing of terrorism. All reporting entities have obligations in respect of the Act to mitigate the risk that the financial and business transactions in which they are engaged are used for the purpose of laundering money or financing terrorism.

2.4.1 Applicability

These Guidelines apply to all reporting entities as defined in Article 4 of the Act who are the subject of control by the Financial Inspectorate. As of the publication date of these Guidelines, the Financial Inspectorate is responsible for supervision over the following reporting entities:

- companies performing certain payment operations services, including money transfers;
- Croatian Post Inc.;
- companies for the issuance of electronic money, branches of companies for the issuance of electronic money from member-states, branches of companies for the issuance of electronic money from third countries and companies for the issuance of electronic money from member-states authorised to directly render services of issuing electronic money in the Republic of Croatia;
- authorised exchange offices;
- pawnshops;
- legal and natural persons performing business in relation to the activities listed hereunder:
    - giving credits or loans, also including: consumers' credits, mortgage loans, factoring and commercial financing, including forfeiting,
    - payment instruments issuance and management (e.g., credit cards and traveller's cheques),
    - issuance of guarantees and security instruments,
    - investment management on behalf of third parties and providing advisory thereof,
    - credit dealings intermediation,
    - trusts or company service providers,
    - trading precious metals and gems and products made of them,
    - trading artistic items and antiques,
    - organising or carrying out auctions,
    - real-estate intermediation.
- legal and natural persons performing matters within the framework of the following professional activities:
    - lawyers, law firms and notaries public,
    - auditing firms and independent auditors,
    - natural and legal persons performing accountancy and tax advisory services.

2.4.1.1 Applicability in third countries

In addition, under article 5 of the Act, there is an obligation for reporting entities that have business units and companies seated in third countries with majority ownership or with predominant decision-making rights exercised by the reporting entities to ensure that money laundering and terrorist financing prevention and detection measures are applied within the equal scope in their business units and companies, unless such a course of action would be in direct contradiction to the legal regulations of the third country. Further details on the requirement for application of the Act extraterritorially are described in section 8 of these Guidelines.

2.4.2. Activities triggering obligations as reporting entities for attorneys at law, law firms and notaries public.

Of the list of reporting entities noted in Section 2.4.1 of these Guidelines, the legislated and regulatory obligations of **attorneys at law, law firms and notaries public are only triggered when they engage in certain activities on the territory of the Republic of Croatia**. For purposes of clarity, attorneys at law and public notaries **proceed according to the Act only when they**:

1. perform a financial transaction or a transaction linked with real estate, on behalf of and for the account of a client,

2. help in planning or performing a transaction for a client connected with:
    a. purchase or selling of a real estate or a share, that is, of stocks of a company,
    b. managing financial funds, securities or other property in client's ownership,
    c. opening or managing bank accounts, savings deposits or accounts for operations with securities,
    d. collecting funds necessary for founding and operating of a company, as well as for its managing,
    e. founding, operating and managing of an institution, fund, company or other similar legal-organizational form.

2.5 The Financial Inspectorate of the Republic of Croatia Act

The Financial Inspectorate of the Republic of Croatia Act (hereafter referred to as the Financial Inspectorate Act or FIA) defines the competence and authority of the Financial Inspectorate in regards to the supervision of the implementation by reporting entities of provisions to prevent money laundering and terrorist financing.

Several critical articles of the FIA are relevant to reporting entities to better understand their own obligations, their own rights and the authority of the Financial Inspectorate in the performance of its role as a supervisor.

2.5.1 The authorities of the Financial Inspectorate and obligations of reporting entities

The Financial Inspectorate is the main supervisor in the Republic of Croatia over the implementation of the money laundering and terrorist financing prevention measures.

Under Articles 9, 10, 11, 12 and 14 of the FIA, the Financial Inspectorate can:

- inspect business records, bank and financial documentation, contracts, business evidence and other documents in any form whatsoever and obtain copies thereof,
- inspect business premises, goods, installations and equipment,
- determine the identity of persons engaged by reporting entities,
- seek information and take statements from persons who have important knowledge for inspection supervision,
- request that reporting entities provide documentation and information for the performance of an examination,
- seek abstinence from all activity that is contrary to the provisions of the law,
- temporarily confiscate objects and documentation, and
- directly examine on the premises of a reporting entity original documentation, monitor, collect and verify data, and obtain information from other sources,
- apply the following measures to reporting entities, on the application of the principle of proportionality:

- issue a written warning to eliminate irregularities,
- order the elimination of illegalities and irregularities,
- propose the suspension of the implementation of financial transactions and the freezing of financial assets,
- temporarily prohibit the undertaking of specific business activities, pursuant to the authorities that issue from the Minor Offence Act, and
- propose the revocation of authorization to work.

2.5.2 Reporting entity obligations in cooperating with the Financial Inspectorate

Under the Act, reporting entities have a number of obligations in collaborating with the Financial Inspectorate. They must:

- deliver information at the request of the Financial Inspectorate (Article10 of the FIA),
- facilitate access by authorized persons of the Financial Inspectorate to the headquarters and other locations where reporting entities conduct business (Article 13 of the FIA),
- facilitate the control of the records and business documentation and administrative or business evidence (Article 13 of the FIA)
- provide suitable premises in which it is possible to perform unhindered supervision, without the presence of other persons (Article 14 of the FIA)
- secure expert and technical assistance and to provide the necessary explanations required for the performance of supervision (Article 14 of the FIA).

While the authorized person of the Financial Inspectorate shall perform the supervision of operations during the working hours of the reporting entity, if the extent or the nature of the work so necessitates, the reporting entity shall be required to make it also possible for the authorized person of the Financial Inspectorate to perform their examination outside of regular working hours (Article 14 of the FIA).

3. Key measures to be taken by reporting entities to implement the Anti-Money Laundering and Terrorist Financing Act

An effective ML/TF prevention and detection regime is one where reporting entities:
- fully comply with their legislated obligations;
- have tailored their business operations to combat ML/TF;
- anti-money laundering and anti-terrorist financing measures are consistently implemented; and
- meet existing international and national anti-money laundering and anti-terrorist financing standards.

In order for reporting entities to better understand and achieve compliance with their Anti-Money Laundering and Terrorist Financing Act obligations, these Guidelines have been grouped in four (4) key categories of measures**.** These categories are as follows:

- Internal controls;
- Customer due diligence;
- On-going monitoring and reporting; and
- Data keeping and record keeping.

Detailed guidance is provided under each of these categories for the requirements that must be met by reporting entities.

4. Internal Controls

4.1 Risk based approach

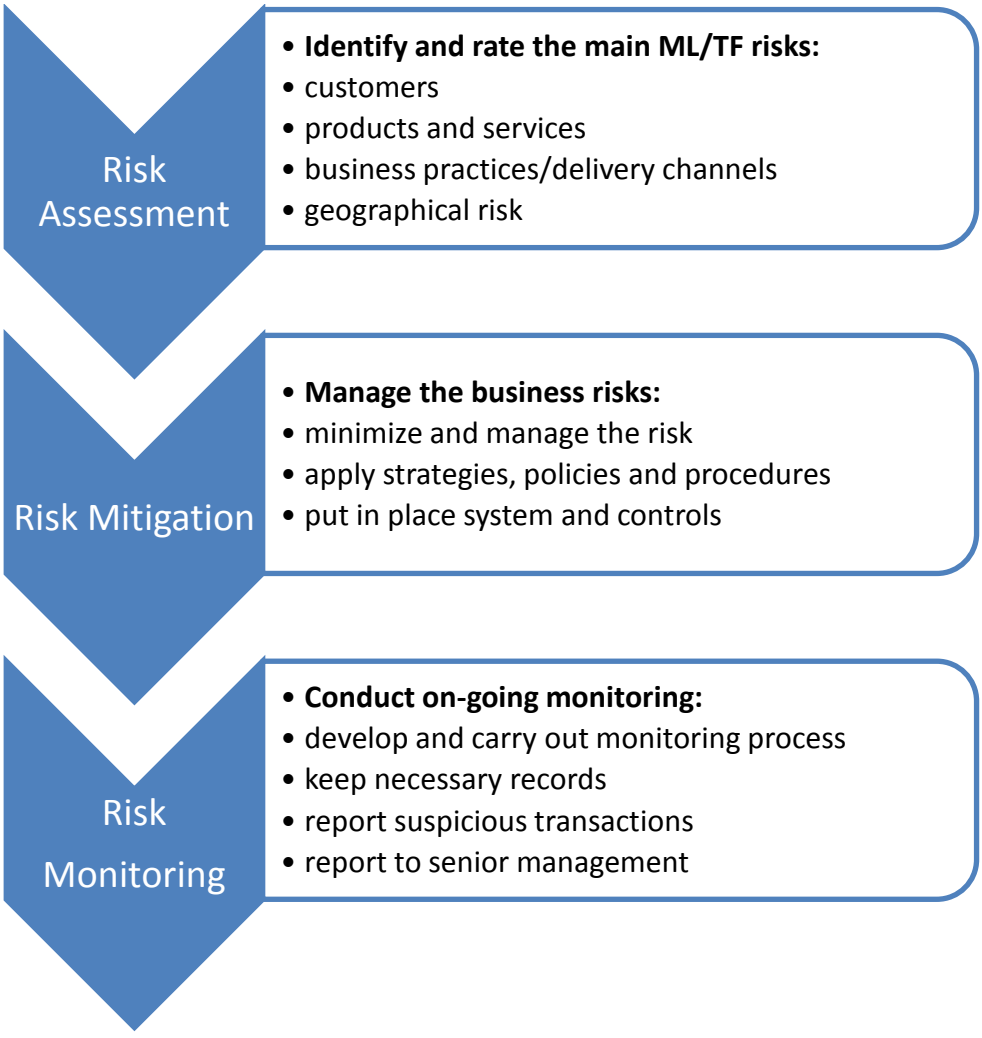
Reporting entities are required to conduct an assessment of and document the risks related to money laundering and terrorist financing. A risk-based approach is a process that allows reporting entities to identify potential high risks of money laundering and terrorist financing and develop strategies to mitigate them. When it comes to situations where enhanced due diligence is appropriate, a principle of risk-based approach will allow reporting entities to focus resources where they are most needed to manage risks within the reporting entity's tolerance level.

The approach to the management of risk and risk-mitigation requires the leadership and engagement of senior management towards the detection and deterrence of money laundering and terrorist financing. Senior management is ultimately responsible for making management decisions related to policies, procedures and processes that mitigate and control the risks of money laundering and terrorist financing within a business.

The scope of applied measures for prevention and detection of money laundering and terrorist financing should be proportional to the identified money laundering and terrorist financing risk degree (risk-based approach).

There are three steps to establishing a risk based approach: risk assessment, risk mitigation and risk monitoring. The following diagram depicts visually the three different steps in implementing a risk based approach.

Diagram 1: Risk Based Approach



4.1.1 Risk assessment

A risk assessment is an analysis of potential threats and vulnerabilities to money laundering and terrorist financing to which the reporting entity's business is exposed. The complexity of the assessment depends on the size and risk factor of the entities' business.

When conducting a risk assessment reporting entities should identify and rate the main ML/TF risks in the following categories:

- customers;
- products and services;
- business practices/delivery channels; and
- geographical.

Customer risk
Reporting entities have to consider the nature and business of their clients to determine the level of risk of money laundering and terrorist financing. In other words, reporting entities have to know their clients to perform a risk assessment. Knowing clients is not limited to identification or record keeping requirements. It is about understanding clients, including their activities, transaction patterns, how they operate and so on. Other elements, such as the magnitude of a client's assets or the number of transactions involved, might also be relevant.

Some reporting entities may choose to conduct a risk assessment for each customer. Others, based on the nature of their business, may choose to group customers by category and conduct a risk assessment on the group of customers. For example, a real estate agent may choose to identify any customer located outside of Croatia as higher risk. An individual assessment of each customer is not required.

Products and services risk
Reporting entities have to be aware of and recognize products and services or combinations of them that may pose higher risks of money laundering or terrorist financing. Legitimate products and services can be used to mask illegal origins of funds, to move funds to finance terrorist acts or to hide the true identity of the actual owner or beneficiary of the product or service. Products and services that can support the movement and conversion of assets into, through and out of the financial system may pose a high risk. In addition, you may also consider services identified by regulators, governmental authorities or other credible sources as being potentially high risk for money laundering or terrorist financing.

Business practices/delivery channels risk
Reporting entities are also required to consider the channels used to deliver their products or services. In today's economy and global market, many delivery channels do not bring the client into direct face-to-face contact with the reporting entity (for example, Internet, telephone or mail), and are accessible 24 hours a day, 7 days a week, from almost anywhere. The remoteness of some of these distribution channels can also be used to obscure the true identity of a client or beneficial owners and can therefore pose higher risks.

Geographical risk
Reporting entities have to consider whether geographic locations in which they operate or undertake activities pose a potentially higher risk for money laundering and terrorist financing. Depending on their business and operations, geographic locations can range from their immediate surroundings, whether rural or urban or other countries.

A checklist in ANNEX 4 provides an example, for use by reporting entities, to facilitate the assessment of the above factors. However, a reporting entity's risk assessment has to be appropriate

for their specific business needs which means that it may have to be more detailed than the checklist provided. Reporting entities can customize the checklist or can use a different method or another tool.

High risk for money laundering and financing of terrorism

Although there is not a generally accepted list of risk categories, examples listed in Annex 3 of these Guidelines are the most commonly used. These potential risks can help you in determining higher risk situations. It should be noted that if you determine that a customer or situation is higher risk you are required to apply risk mitigations measures and enhanced due diligence. You are **not** required to refuse the transaction or end the business relationship.

Moderate risk for money laundering and financing of terrorism
Clients of moderate risk are those that cannot be categorized as of high or low risk.

Low risk for money laundering and financing of terrorism
According to Article 35 the Act, low risk clients are the following:

- Banks, branches of foreign banks and banks from Member States authorized for the direct provision of banking services in the Republic of Croatia, savings banks, housing savings banks,
- Companies performing certain payment operations services, including money transfers, the Croatian Post (Hrvatska Pošta d.d.), investment funds management companies, business units of third country management companies, management companies from Member States having a business unit in the Republic of Croatia and authorized to directly perform fund management business on the territory of the Republic of Croatia and third persons which are allowed, according to the law regulating the operation of funds, to be entrusted with certain tasks by the respective management company, pension companies, companies authorized to do business with securities and branches of foreign companies dealing with securities in the Republic of Croatia; or other identical institution, under the condition that it has headquarters in the Member State or equal third country from Article 25, paragraph 5 of the Act,
- State bodies, local and regional self-government bodies, public agencies, public funds, public bureaus or chambers,
- Companies the securities of which are accepted and used for trading on the capital market in one or more Member States according to legal regulations which are put in force in the European Union, or companies with headquarters in a third country the securities of which are accepted and used for trading on the capital market in a Member State or in this third country, under the condition that that country requests the uncovering of data according to legal regulations of the European Union area.

Reporting entities can put in the category of clients representing a negligible risk of money laundering or financing of terrorism, only those clients that meet the conditions from the Ordinance on the determination of the conditions under which the reporting entities categorize clients in clients representing a negligible risk of money laundering or financing of terrorism ("Official Gazette", 76/09).

Variables that can have an impact on the risk

Reporting entities should take into account the peculiarities, the risk degree or suspiciousness of a transaction or a recommended business relationship. Therefore, the risk assessment procedure can also contain variable risks which are specific for a certain client or a type of business. The existence of one or more variables can result in the implementation of an enhanced due diligence and in the necessity to monitor, or a usual due diligence and monitoring can be reduced or simplified. The following ones are variables which can have an impact on increasing or decreasing of the risk of certain client or type of business:

- nature of a business relationship with a client and the existence of specific activities,
- level of legislation or the existence of the supervision by competent bodies. For example, clients who are subject to a satisfactory system of preventing money laundering and financing of terrorism represent a lower risk than clients from the industry where there is a risk of money laundering because they are not regulated for the purpose of preventing these activities,
- reputation and publicly available information on the client. Legal persons which are transparent and well known in the public domain and which are in operation for many years without verdicts being delivered against them (offences linked with illegally acquired property) represent a low risk of money laundering,
- regularity or duration of a business relationship,
- knowledge of the client's country including the knowledge of local laws, regulations and rules, as well as the structure and scope of a regulatory supervision,
- proportionality between the size or scope and longevity of client's doing business including the nature of requested service,
- significant or unexplainable geographic distance between an attorney at law or a public notary and a client, when there is no need for that,
- a person who could become a client orders to an attorney or to a public notary to carry out only one transaction (more risky than a continuous advisory relationship),
- risks resulting from the use of new technology which enables a business relationship without the client's presence (non-face to face) and which favours anonymity,
- when a future client is recommended by a person of confidence who is a subject to the AMLFT regime which is in accordance to the FATF standards, the recommendation can be considered as a mitigating risk factor,
- structure of a client or a transaction. Structures without visible legal, tax, business, economic or other legislative purpose may increase the risk.

4.1.1.1 Assessment criteria

When determining whether a reporting entity has adequately implemented risk assessment measures the following criteria will be evaluated:

The risk assessment strategies are documented - It is important that the risk assessment strategies developed by the reporting entity are documented. This allows the risk assessment strategies to be shared with management and employees.

The risk assessments are proportionate - Due regard must be accorded to the vast and profound differences in practices, size, scale and expertise, amongst reporting entities. As a result, consideration must be given to these factors when evaluating a reporting entity's risk assessment and mitigation strategies.

The risk assessment can take different forms depending on the size and operations of the reporting entity. A checklist may be appropriate for a small firm but a more comprehensive document including a risk matrix may be appropriate for larger entities.

The risk assessment should take into account key risk elements - An entity's risk assessment should be comprised, at a minimum of the following elements:

- **Customer risk –** The reporting entity should consider the nature and business of its customers and their business relationships to determine the level of ML/FT risk associated with each type of customer or business relationship. It should be noted that conducting a risk assessment of each individual customer is not required. Examples of customer risk are included in Annex 3.

- **Product/services** - An overall risk assessment should include determining the potential risks associated with the services offered by the reporting entity noting that various reporting entities provide a broad and diverse range of services. The context of the services being offered is always fundamental to a risk-based approach. Examples of product/service risk are included in Annex 3.
- **Business practices/delivery channels –** The reporting entity should consider the channels used to deliver their products and services. Many delivery channels do not bring the customer into direct face to face contact with the customer. Attention should be paid to the remoteness of distribution channels as they can also be used to obscure the true identity of a client or beneficial owners and can therefore pose higher risks. Examples of business practices/delivery channels risk are included in Annex 3.
- **Geographical risk –** The reporting entity should consider whether the geographic locations in which it operates, undertakes activities or where a client is located poses a potentially higher risk for ML/FT. Examples of geographical risk are included in Annex 3.

The risk assessment strategies are reviewed by senior management annually – Strong senior management leadership and engagement in AML/CFT is an important aspect of the application of the risk-based approach. Senior management should approve the risk assessment strategies and ensure that they are reviewed annually.

The risk assessment strategies are shared with employees - For a risk management framework to be effective employees need to be aware of those situations that have been identified as high risk.

Low risk clients are identified – In conducting the risk assessment the reporting entity can identify types of customers that are considered low risk as defined by Article 35, the rule book, and as described in Annex 3 of these Guidelines.

4.1.2 Risk mitigation

Risk mitigation is about implementing measures to limit the potential money laundering and terrorist financing risks the reporting entity has identified while staying within its risk tolerance level. As part of its internal enactment, when the risk assessment determines that risks are high for ML or FT, the reporting entity has to develop written risk mitigation strategies (policies and procedures designed to mitigate high risk) and apply them for high risk situations. Annex 5 provides a list of risk mitigation measures that may be appropriate for situations that you have determined to be high risk.

4.1.2.2 Assessment criteria

When determining whether a reporting entity has adequately implemented risk mitigation measures the following criteria will be evaluated:

The risk mitigation strategies are documented - It is important that the risk mitigation strategies developed by the reporting entity are documented. This allows the risk mitigation strategies to be shared with management and employees. Furthermore, the application of the mitigation strategies should be recorded to demonstrate that mitigation measures have been applied.

The risk mitigation strategies are reviewed by senior management annually – Strong senior management leadership and engagement in AML/CFT is an important aspect of the application of the risk-based approach. Senior management should approve the risk mitigations strategies and ensure that they are reviewed annually.

The risk mitigation strategies are shared with employees - This will allow employees to apply risk mitigation measures established by the authorised person or his/her Deputy as per Article 46 of the Act.

4.1.3 Risk monitoring

In addition to risk assessment and risk mitigation activities the Act also requires reporting entities to take measures to conduct on-going monitoring of financial transactions. The level of monitoring should be adapted according the ML/TF risks as outlined in the entity's risk assessment. The purpose of on-going monitoring activities is to help detect suspicious transactions.

The reporting entity's internal enactment has to determine what kind of monitoring is done for particular high risk situations, including how to detect suspicious transactions. The internal enactment should also describe when monitoring is done (its frequency), how it is reviewed, and how it will be consistently applied. Section 6.2 of these Guidelines also discusses other monitoring obligations and how monitoring activities can be conducted.

4.1.3.1 Assessment criteria

When determining whether a reporting entity has adequately implemented risk monitoring measures the following criteria will be evaluated:

A monitoring schedule is developed – Reporting entities should review transactions based on an approved schedule that involves management sign-off.

Changes in activities are documented – The reporting entity should flag changes in activities that is contrary to normal transaction patterns or client activities. A process is in place to elevate concerns as necessary.

Monitoring parameters are established – Reporting entities should set business limits or parameters regarding transactions that would trigger early warning signals and require mandatory review. Operational documents demonstrate that the policy is effectively applied.

High risk transactions or relationships are monitored more frequently – Reporting entities review high risk transactions more frequently against suspicious transaction indicators relevant to the relationship and escalate them should additional indicators be detected.

Monitoring activities take into account the purpose of the business relationships and the intended source of funds – When conducting on-going monitoring the reporting entity should refer to purpose of the business relationship and intended source of funds that was documented at the beginning of the business relationship to ensure that activities correspond to what was stated by the client.

Suspicious transactions are reported to the FIU – The purpose of on-going monitoring activities is to identify suspicious transactions. Transactions that are identified by entities as being suspicious during monitoring activities should be reported to the FIU. Although a strictly quantitative analysis of the number of STRs reported would not be appropriate given the varying levels of ML/FT risk in each reporting entity sector, the number of suspicious transactions detected can potentially be an indicator of an effective monitoring program.

4.2 Internal enactment

All reporting entities are obliged, according to Article 48 of the Act, to issue an internal act establishing measures, actions and proceedings for the prevention and detection of money laundering and financing of terrorism, prescribed by the Act and regulations passed on its basis.

In accordance with the provisions of Article 48 of the Act, an internal act will provide for measures, actions and procedures to prevent and detect ML/TF.

The internal act should include, among other requirements, all of the following:

- a determination of the responsibility of the compliance officer (authorized persons) and the reporting entity's employees in implementing this Act (mandatory as per Article 48);
- procedures for determining foreign politically exposed persons (PEP) (mandatory as per Article 32);
- procedures of the implementation of client due diligence measures (mandatory as per Article 8);
- procedures for the development, application and maintenance of an indicators list (mandatory as per Article 41);
- a description of the implementation of internal procedures referring to the prevention of money laundering and financing of terrorism and specifically:
    - the development and implementation of professional training and education of employees;
    - risk assessment, risk mitigation and monitoring procedures;
    - the procedures of verifying client identification (ID), of reporting to competent bodies, and other procedures;
    - how to detect suspicious transactions;
    - the way of reporting to the Office;
    - the manner in which records are kept on collected data;
    - determination of the kind of monitoring for particular high risk situations;
    - when risk monitoring is done (its frequency), how it is reviewed, and how it will be consistently applied;
    - the scheduling and implementation of the annual internal audit of the performance of ML/TF prevention and detection measures;
    - rrecord keeping requirements: manner and deadlines for keeping data, protection of data, content and method of record keeping;
    - detection and reporting of prescribed transactions to the FIU;
    - internal audit: the frequency and manner in which internal audits are conducted; and
    - procedures for senior management' annual review and approval of the risk assessment and mitigations strategies**.**

4.2.1 Assessment criteria

The internal enactment is documented – All internal enactments should be documented.

The internal enactment addresses all the prescribed measures – The internal enactment should provide a complete overview of how the reporting entity is to comply with AML/CFT obligations. All internal enactments should include the measures listed in Section 4.2 of these Guidelines.

The policies and procedures are implemented – Reporting entities are to ensure that the staff applies, in the ordinary course of business, all measures and actions prescribed in the internal enactment for detecting and preventing ML/FT.

The employees are knowledgeable about policies and procedures – For policies and procedures to be effective employees need to be knowledgeable about the policies and procedures and how they affect their day to day activities.

The suspicious transactions are identified and reported – The reporting entity's policies and procedures are effective in identifying and reporting suspicious transactions.

The training is delivered –The reporting entity's employees have received training and are knowledgeable with respect to the policies and procedures, ML/TF trends and typologies and risks that exist within the reporting entity.

The internal enactment is proportional – The internal enactment should be adapted to the practices, size, scale and expertise of the reporting entity.

4.3 Appointment of a compliance officer

The Act designates an authorized person (hereafter referred to as the compliance officer) as responsible for carrying out measures and tasks in relation to the Act and its regulations. Pursuant to Article 44 paragraph 2 of the Act, reporting entities, with exceptions noted in Section 4.3.1 of these Guidelines, are obliged to appoint a compliance officer and his/her deputy in a written form. When it is not possible to appoint such a person, the legal representative or the other person in charge or running the arrangements of the reporting entity shall be deemed to be a compliance officer.

Reporting entities are obliged to inform the Anti-Money Laundering Office (AMLO) about the appointment of the compliance officer immediately and no later than 7 days after the appointment, i.e., change of data regarding the compliance officer.

Furthermore, pursuant to Article 47 of the Act reporting entities must establish certain work conditions for the reporting entity's compliance officer to meet their obligations such as providing:

- unrestricted access to all data, information and documentation necessary for the purposes of money laundering and terrorist financing prevention and detection;
- adequate authorizations for an efficient conduct of tasks referred to in Article 46, paragraph 1 of the Act;
- adequate human resource, material and other work conditions;
- adequate premises and technical conditions guaranteeing a proper degree of data confidentiality and information protection available to the compliance officer;
- adequate IT support enabling on-going and safe monitoring field the activities in respect of money laundering and terrorist financing prevention and detection;
- regular professional training in relation to money laundering and terrorist financing prevention and detection; and
- replacement of the compliance officer during their absence.

4.3.1 Exceptions to the appointment of a compliance officer

Persons involved in professional activities, specifically attorneys at law, public notaries, auditing firms, independent auditors, accountancy and tax advisory services are exempted under Article 55, paragraph 3, item 3 of the Act from having to appoint a compliance officer.

4.3.2. Assessment criteria

A compliance officer is appointed - The reporting entity has appointed the compliance officer/deputy, who are responsible for carrying out AMLCFT measures and tasks.

The AMLO is informed of compliance officer appointment - The reporting entity has informed the AMLO immediately or no later than within 7 days after the appointment or change of data.

The compliance officer meets all prescribed criteria – The tasks falling under the remit of the appointed person and its deputy, are performed solely by persons who meet the requirements prescribed by Article 45 of the Act. These include:

- The compliance officer has a senior position within the organization;
- The compliance office has independence in his/her work;
- The compliance officer has direct lines of communication with management;
- The compliance officer does not have a criminal record or is not subject to criminal proceedings;
- The compliance officer has been trained with respect to his/her responsibilities; and

- The compliance officer is familiar with the nature of the reporting entity's operations.

The compliance officer completes all prescribed tasks – The tasks outlined in Article 46 of the Act are conducted. These tasks include:

- Developing and implementing the AML/CFT prevention and detection system for the reporting entity;
- Providing timely information to the AMLO;
- Designing internal enactment that includes policies and operational procedures to comply with AML/CFT requirements;
- Monitoring and coordinating the REs AML/CFT prevention and detection activities;
- Establishing IT support mechanisms for AML/CFT detection;
- Making suggestions to the Board or managerial body on improving the prevention and detection of AML/CFT; and
- Producing and overseeing the delivery of professional improvement and training programs for AML/CFT.

The reporting entity meets its obligations towards its compliance officer – The reporting entity is required under Article 46 to establish favorable conditions for the compliance officer to complete its duties. These conditions can be found at Section 4.3 of these Guidelines.

4.4 Training

All reporting entities are obliged, according to Article 49 of the Act, to ensure regular professional education and training of their staff to prevent and detect money laundering and the financing of terrorism.

Professional education and training provide the familiarization with the provisions of the Act and ordinances for its enforcement, internal acts, international standards deriving from international conventions on the prevention of money laundering and financing of terrorism, guidelines, lists of indicators for recognizing suspicious transactions, reporting and record-keeping obligations.

Reporting entities a programme for the annual professional education and training of employees for the prevention and detection of money laundering and financing of terrorism.

In addition, Article 78 of the Act prescribes that reporting entities must keep and store data and documentation pertaining to the professional training they have provided for four years after the professional training has been delivered.

4.4.1 Assessment criteria

The training program is documented - The training program should be documented. It should describe the content of the training, when the training was delivered and who participated in the training. The date that the training program has been reviewed should also be documented including any changes that have been made to the training program.

The training program is proportional to the size of the business – Reporting entities should design, develop, implement and update their training program as appropriate to the nature and size of their business. Training can be delivered through presentations, written documentation or through an on-line training program.

The training program is proportional to the level of ML/FT risk - A reporting entity's training program must also be adapted to the ML/FT risk. Not only does it mean that the content of the training should be focused on the particular vulnerabilities that are specific to the business' activities but also that entities that are at a higher risk of being used for ML/FT should have a more tailored training program targeted to the identified risks.

The training is comprehensive – The content of the training should provide employees and management of the firm a clear understanding of their responsibilities vis-à-vis AML/CFT obligations and an overview of vulnerabilities linked to this business' operations. Specifically the training program should include information on ML/TF techniques, methods and trends, an explanation of AML/CFT laws and regulations, an overview of customer due diligence, record keeping and reporting requirements, a review of the entity's policies and procedures, risk assessment and risk mitigation strategies.

The training is delivered at least annually – Training should be delivered at least annually. Training should be delivered more frequently if there are changes in the business practices or when there are changes to reporting entity obligations.

The training is delivered to all employees – All reporting entity employees should be subject to AML/CFT training to ensure that business processes are explained and AML/CFT policies, procedures and risks are understood.

New employees should be trained prior to interacting with clients - AML/CFT training should be integrated within an employee's initial orientation. The training should be completed by the new employee prior to interacting with clients.

The training program is reviewed annually- The training program should be reviewed at a minimum on an annual basis. A review of the training program should be undertaken each time there are changes in the business processes or when legislative or regulatory amendments have been adopted.

4.5 Internal audit

Pursuant to Article 50 of the Act, with the exception of reporting entities noted in Section 4.5.1 of these Guidelines, all other reporting entities must ensure that a regular internal review to test the appropriateness and effectiveness of their policies and procedures, risk assessment and training program is conducted at least once a year.

The review can be conducted by an internal or external auditor. If the reporting entity does not have an auditor, it can conduct a "self-review". The self-review should be conducted by an individual who is independent of the reporting, record keeping and compliance-monitoring functions. This could be an employee or an outside consultant. The objective of a self-review is similar to the objectives of a review conducted by internal or external auditors. It should address whether policies and procedures are in place and are being adhered to, and whether procedures and practices comply with legislative and regulatory requirements.

4.5.1 Exceptions to carrying out an internal audit

Persons involved in professional activities, specifically attorneys at law, public notaries, auditing firms, independent auditors, accountancy and tax advisory services are exempted under Article 55, paragraph 3, item 3 from having to carry out an internal audit over the performance of ML/TF related tasks.

4.5.2 Assessment criteria

Internal audit is documented – The internal audit is documented and includes the specific areas reviewed by the auditor or the person conducting the review, the date that the audit/review was undertaken and the recommendations that were put forth.

Internal audit is proportional to the size of business – As with the other elements of the compliance regime the internal audit should take into account the size of the business. Large

businesses such as international corporations or large businesses business should conduct a more comprehensive audit conducted by an independent auditor. As mentioned previously in this section smaller entities can consider conducting a self-review.

Internal audit is comprehensive - The internal audit should be comprehensive and include an analysis of the entity's policies and procedures, training program and risk management framework. When examining the risk management framework the internal auditor should have reviewed all elements including the risk assessment, risk mitigation strategies and risk monitoring procedures.

The review by the internal auditor should include interviews, tests and samplings such as the following:

- interviews with those handling transactions and with their supervisors to determine their knowledge of the legislative requirements and your policies and procedures,
- a review of the criteria and processes for identifying and reporting suspicious transactions,
- a test of the record keeping system for compliance with the legislation,
- a test of the client identification procedures for compliance with the legislation,
- a review of the risk assessment, and
- any other elements prescribed by by-law.

Internal audit should be conducted on an annual basis - The audit or review should be conducted at least once a year.

Results of the internal audit are reported to senior management – The results of the audit/review should be reported within a reasonable timeframe of the audit/review being completed. The report should include the results of audit/review, any updates that were made to the policies and procedures during the review period and the status of implementation of the policies and procedures. Any deficiencies should be identified and also reported to senior management or the board of directors. The report should also include a request for response indicating corrective actions and a timeline for implementing such actions. The date that the audit results were presented to senior management and the management response to the audit should be documented.

5. Customer Due Diligence

With one exception for persons engaged in professional activities, reporting entities have obligations under Article 8 of the Act for implementing customer due diligence measures.

Under this article, due diligence encompasses the following measures:

1. identifying the customer and verifying the customer's identity on the basis of documents, data or information obtained from a credible, reliable and independent source;
2. identifying the beneficial owner of the customer and verifying beneficial owner's identity;
3. obtaining information on the purpose and intended nature of the business relationship or transaction and other data in line with this Law;
4. conducting on-going monitoring of the business relationship including due scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the reporting entity's knowledge of the customer, the type of business and risk, including, as necessary, information on the source of funds, in which the documents and data available to the reporting entity must be kept up-to-date.

When determining the beneficial ownership of a legal entity, the reporting entity can consult corporate registries, articles of incorporation or other publicly available information. The entity can also ask the

individual representing the legal entity the information about the beneficial owner. The efforts to determine the beneficial owner should be documented. In the event that the beneficial owner cannot be determined, the entity should consider the relationship or transaction as being higher risk and apply risk mitigation measures as well as consider the appropriateness of reporting to the AMLO.

When determining the source of funds and property, the reporting entity can consult publicly available information or directly ask the client. The efforts to determine the source of funds and property should be documented. In the event that the source of funds cannot be determined, the entity should consider the relationship or transaction as higher risk and apply risk mitigation measures as well as consider the appropriateness of reporting to the AMLO.

Customer Due Diligence Exception for Professionals: Pursuant to Article 53 of the Act customer due diligence requirements shall not apply to the persons involved in the performance of professional activities in respect of information they receive from or obtain on a customer during the course of establishing the legal position of the customer or during the representation of the customer in relation with a court proceeding which shall include advice on proposing or avoiding court proceeding, whether such information is received or obtained before, during or after the completion of such court proceedings.

Guidance note for lawyers, law firms and notaries public on what will be examined by the Financial Inspectorate.

In conducting examination in offices of lawyers and notaries public the Financial Inspectorate will focus on the lawyer's and notary's role in assisting in the planning or conducting of financial and real estate transactions. This may involve situations involving the Land Registry or Commercial Court, the final determination to be made based on the facts of each individual situation.

The examination will concentrate on the review of documents that demonstrate that the entity has complied with AML/CFT obligations. The Inspectorate will not request documents that are subject to solicitor-client privilege. It is suggested that lawyers and notaries public keep information related to AML/CFT requirements separate in order to ensure the integrity of privileged information.

5.1 Circumstances where customer identification and verification is required

The Act prescribes in Article 9 the reporting entities shall be obliged to conduct customer due diligence in the following cases:

1. when establishing a business relationship with a customer;
2. when carrying out each transaction amounting to HRK 105,000 or more (a single operation or several linked transactions totalling more than HRK 105,000);
3. when there are doubts about the credibility and veracity of the previously obtained customer or customer beneficial owner information;
4. in all instances when there are reasons for suspicion of money laundering or terrorist financing in relation to a transaction or a customer, regardless of the transaction value.

With transactions of HRK 105,000 or more performed on the basis of a previously established business relationship with the reporting entity, in conducting customer due diligence the reporting entity shall only verify the identity of the customer.

Before establishing a business relationship with a customer, the reporting entity must engage in the following three activities:

1. identify the customer and verify the customer's identity on the basis of documents, data or information obtained from a credible, reliable and independent source;
2. identify the beneficial owner of the customer and verify the beneficial owner's identity; and

3. obtain information on the purpose and intended nature of the business relationship or transaction and other data in line with the Act.

Reporting entities may also conduct customer due diligence **during** the establishment of a business relationship with a customer, should it be necessary not to interrupt the usual manner of establishing business relationships and there is a negligible risk of money laundering or terrorist financing. In instances where customer due diligence is not conducted prior to the establishment of the business relationship, the reporting entity should document why the customer due diligence could not be completed prior to establishing the business relationship and the nature of the transactions that was conducted. Customer due diligence should be conducted as soon as practicable and no later than 3 days after the establishment of the business relationship.

5.1.1 Assessment criteria

Customer due diligence is conducted prior to establishment of business relationship - the reporting entity is obliged to carry out prescribed measures prior to the establishment of a business relationship.

Customer due diligence is conducted during the establishment of business relationship on an exception basis - the reporting entity, may also conduct the measures during the establishment of a business relationship with a customer, should it be necessary not to interrupt the usual manner of establishing business relationships and if pursuant to Article 7 of the Act there is a negligible risk of money laundering or terrorist financing.

Customer due diligence is conducted for transactions amounting to HRK 105,000 - the reporting entity is obliged to carry out due diligence measures when carrying out each transaction amounting to HRK 105,000 or more, whether the transaction is carried out in a single operation or several transactions which appear.

Prior to carrying out the transactions - the reporting entity is obliged to carry out prescribed measures prior to the carrying out the transactions.

CDD is conducted when there are doubts about credibility and veracity. Customer due diligence is conducted when there are doubts about the credibility and veracity of the previously obtained customer or customer beneficial owner information.

CDD is conducted when there is a suspicion. Reporting entities should conduct customer due diligence in all instances when there are reasons for suspicion of money laundering or terrorist financing in relation to a transaction or a customer, regardless of the transaction value.

5.2 Measures to conduct customer due diligence

5.2.1 Measure for identifying the customer and verifying the customer's identity

The reporting entity must identify and verify the identity of a customer which is a natural person and natural person's legal representative, a sole proprietor or a person involved in carrying out other independent business activity through the collection of data referred to in Article 17 of the Act through the examination of the official customer's personal identification document in customer's presence, from other valid public documents submitted by the customer, i.e. directly from the customer, from the customer's written statement or otherwise if prescribed by the Minister of Finance in a bylaw.

In instances when the customer is a sole proprietor or a person involved in the performance of other independent business activity, with a given identification number, the reporting entity shall collect

data in keeping with the provisions contained in Article 16, Paragraph 1 item 5 and article 18 of the Act.

The reporting entity identifies and verifies the identity of a customer which is a natural person and natural person's legal representative, a sole proprietor or a person involved in carrying out other independent business activity through the collection of data referred to in Article 17 of the Act through the examination of official customer's personal identification document in customer's presence, from other valid public documents submitted by the customer, i.e. directly from the customer, from customer's written statement or otherwise if prescribed by the Minister of Finance in a bylaw.

5.2.1 Assessment criteria

Natural persons are identified and the identity is verified - Reporting entity identifies natural persons and verifies their identity.
Correct identification data is collected - For natural persons - name and surname, permanent address, date of birth, place of birth, personal identification number, name and number of the identification document issuing entity.

Legal Persons are identified and the Legal Person's identity is verified. The reporting entity identifies the customer and verifies the customer's identity by examining the original or notarized photocopy of documentation from court or other public register presented by the legal person's legal representative or person authorized by power of attorney (must not be more than 3 months old)[7] through a direct examination of court or other public registers, from written statement from the legal representative or the person authorized by power of attorney. Should the customer be a legal person performing business activity in the Republic of Croatia through its business unit – a branch, the reporting entity shall identify the foreign legal person and its branch and verify their respective identities.

Correct information is collected on legal entities. The reporting entity should collect the following data about legal person: name, seat (street and number, place and country) and business registration number (for a legal person, whereas the registration number is to be included for a craftsman or a person carrying out other independent business activity if such a number has been assigned to such a person).

Identifying a legal person's legal representative and verifying the legal representative's identity. The reporting entity shall identify a legal person's legal representative and verify the legal representative's identity through examination of a personal identification document of the legal representative in his/her presence, from other valid public document supplied by the legal representative or from a written statement from the legal representative.

Correct information is collected about legal representatives. Reporting entities should collect the following data about the legal representative: For legal representatives - name and surname, permanent address, date of birth, place of birth, personal identification number, name and number of the identification document issuing entity.
Identifying and verifying the identity of the person authorized by power of attorney. The reporting entity shall identify and verify the identity of the person authorized by power of attorney by collecting data through the examination of an official personal identification document of the person authorized by power of attorney in his/her presence.

Correct information is collected with respect to power of attorney. The reporting entity should collect data on the customer on whose behalf the person authorized by power of attorney acts, which data shall be collected on the basis of the notarized power of attorney and personal data about person

[7] For the persons involved in performing professional activities- not older than 6 months

authorized by power of attorney.

Identifying other legal persons and entities made equal to them and verifying their identities. In cases of NGOs, endowments and foundations and other legal persons who do not perform economic activity, as well as in cases of religious communities and NGOs without properties of a legal person and other entities without legal personality but independently appearing in legal transactions, the reporting entity is obliged to:

- identify the person authorized to represent, i.e. a representative and verify representative's identity;
- obtain a power of attorney (notarized written authorization) for representation purposes.

Correct information is collected for all situations. Reporting entities should collect:

- For all situations - name and surname, permanent address, date of birth, place of birth, personal identification number, name and number of the identification document issuing entity;
- For natural persons - name and surname, permanent address, date of birth, place of birth of natural person who is a member of another legal person and an entity related;
- For legal persons - name and seat of other legal persons and entities made equal to them as referred to in Article 21 of the Act.

Correct information is collected with respect to powers of attorney for NPOs. Within the framework of customer identification, the persons involved in the performance of professional activities shall identify the customer, i.e. customer's legal representative or the person authorized by power of attorney and shall gather information through the examination of a customer's official personal identification document, i.e. original documents or notarized photocopies of documents or notarized documentation from a court or other public register, which may not be more than three months old.

Additional due diligence

Reporting entities are required to take additional due diligence measures in a number of situations. For specific details reporting entities should refer to the assessment criteria below and the Act. In summary they include the following:

1. collecting information on the purpose and intended nature of the business relationship or transaction;
2. identifying beneficial owners;
3. non face-to-face identification;
4. originator information in Electronic Fund Transfers;
5. refusal to establish business relationship or conduct a transaction; and
6. customer due diligence conducted through third party.

5.3.1 Assessment criteria

Information on purpose and intended nature is collected in prescribed circumstances. Reporting entities shall collect information referred to in Article 25 of the Act at establishing business relationship, at each transaction totaling HRK 105,000 and more, regardless of whether the transaction is made as a single operation or as several transactions which are apparently linked, when there is suspicion as to the credibility and veracity of the previously collected information on customers or the beneficial owner and in all instances when there are reasons to have suspicion of money laundering or terrorist financing associated with a transaction or a customer**.**

Beneficial owners are identified. The reporting entity must identify the customer's beneficial owner which is a legal person, a representative office, a branch, another entity subject to domestic or foreign law made equal with a legal person pursuant to art. 24. of the AML/CFT Law.

Correct information is collected on beneficial owners. The reporting entity must collect the following data on the beneficial owner: name and surname, permanent address, date of birth and place of birth.

Additional client identification measures are applied during non-face-to-face transactions. If the customer was not physically present with the reporting entity during the identification and identity verification, the reporting entity shall be obliged to conduct one or more additional measures pursuant to Article 33.

Originator information is contained in Electronic Fund Transfers. Payment service providers shall be obliged to collect accurate and complete data on the payee and include them in a form or a message accompanying the wire transfer, sent or received in any currency. In doing so, data must follow the transfer at all times throughout the course of the chain of payment.

Payment service providers refuse transaction or ask for additional data when originator information is not contained in Electronic Funds Transfer. The payment service provider shall refuse wire transfers failing to contain complete data on the payee or shall ask for payee data supplement within a given deadline.

Payment service providers terminate relationship when originator information is not included. The reporting entity (credit or financial institution, payment service provider) while conducting electronic money transfer have limited or terminated business relationship with credit institutions and financial institutions (sender of electronic transfer), that failed to collect and include certain information about the origin of transferred money pursuant to Article 15 of the Act (accurate and valid information about the payer).

Payment service providers apply enhanced due diligence when originator information is absent. The payment service provider shall consider a lack of payee information in relation to the assessed level of risk as a possible reason for implementing enhanced transactions due diligence measures.

Business relationship is terminated when customer due diligence is not completed. The authorized person is obliged to examine whether the reporting entity, in case when unable to conduct prescribed measures, terminated established business relationship or carried out transaction, i.e. such a reporting entity must terminate the already established business relationship.

The AMLO is notified when a relationship is terminated. The subject has notified the FIU of the refusal or termination of a business relationship and the refusal to conduct a transaction with all customers of transaction data collected to date in line with Article 13 the Act.

Third party conducting customer due diligence meets all requirements. The reporting entity must determine whether or not the third party who shall be entrusted with the conducting of customer due diligence measures meets all requirements prescribed by the AML/CFT Law.

Note: The Minister of Finance has prescribed in a bylaw issued on June 18, 2009 who may be a third person, terms and conditions under which the reporting entity shall be allowed to entrust the conducting of customer due diligence with a third person, the manner in which the reporting entity shall be enabled to obtain data and documentation prescribed in the Act from a third person, and instances in which the reporting entity shall not be permitted to entrust a third person with conducting customer due diligence.

Customer due diligence conducted by third party is face-to-face. The reporting entity shall not be permitted to accept customer due diligence conducted by a third party on behalf of the reporting entity as adequate, if the third party conducted the identification and identity verification measure within the due diligence exercise without customer's presence.

Customer due diligence conducted by third party is documented and readily available. The reporting entity should have access to customer due diligence information from the third party.

Customer due diligence is not conducted by third party in prescribed circumstances. Reporting entities are prohibited from using third parties to conduct customer due diligence in certain circumstances outlined in Article 5 of the by-law issued on June 18, 2009.

5.4 Politically exposed persons (PEP)

A politically exposed person**,** according to the Act, is every natural person with domicile or habitual residence in a foreign country, who is or was for the last year (or longer) holding a significant public service position, including the members of his/her immediate family or persons known for being his/her close associates.

Natural persons who are holding or were holding a significant public service position are the following ones:

a) presidents of countries, presidents of governments, ministers and their deputies,
b) elected members of legislative bodies,
c) judges of supreme and constitutional and other high courts against whose verdicts, except in exceptional cases, it is not possible to use legal remedies,
d) judges of financial courts and members of central banks councils
e) ambassadors, consuls and senior officers of the armed forces,
f) members of management and supervision boards of legal persons owned by or in the majority ownership of a country.

Members of immediate family, according to the Act are: married or unmarried partners, parents, brothers and sisters, and children and their married and unmarried partners.

A close associate is, according to the Act, every natural person having a common profit from the property or from the established business relationship, or with whom a foreign politically exposed person has other close business contacts.

In determining whether a person is a PEP the reporting entity can consult commercial databases or can ask the customer if he/she falls into the PEP category/definition. The determination of whether the customer is a PEP should be documented.

5.4.1 Assessment criteria

PEPs determination is conducted and documented in prescribed situations. Reporting entities are required to determine the existence of a PEP and document their determination.

Senior management approves business relationship with PEPs. Reporting entities should have procedures for the establishment of business relationships with PEPs including management's role in the approval and on-going risk-based monitoring of PEP relationships.

Enhanced due diligence is conducted when the customer is a PEP. Reporting entities are required to implement enhanced due diligence measures when the customer is a PEP.

5.5 Special forms of customer due diligence

5.5.1 Enhanced due diligence

While the reporting entity must apply customer due diligence measures, some situations require the application of enhanced due diligence measures in a manner and in cases prescribed by the Act. Enhanced customer due diligence, must be applied when certain situations arise such as:

1) the establishment of a business relationship or the conducting of a transaction referred with a politically exposed person, and
2) in instances when the customer was not present in person during identification and identity verification in the course of applying due diligence measures.

The reporting entity may also apply enhanced due diligence when the reporting entity deems that the risk of money-laundering or terrorist financing is greater due to the nature of the business relationship, the form and manner of execution of the transaction execution, the business profile of the customer or other circumstances associated with the customer. Reporting entities shall apply enhanced due diligence measures in the following cases:

Politically exposed persons - the establishment of a business relationship or the conduct of a transaction with a customer who is a politically exposed person;
Non-face-to-face - in instances when the customer was not present in person during identification and identity verification of the person during the course of due diligence measures application (non face-to-face);
Absence of originator information- in instances where originator information is not included in a wire transfer**;**
New technologies – in instances when new technologies that provides anonymity are used. These can include: stored value cards, wire transfers through mobile telephone, etc.;
Higher ML/TF risk - The reporting entity shall apply customer due diligence measures in circumstances that are deemed high risk according to the reporting entity's risk assessment.

Enhanced due diligence measures include the risk mitigation strategies listed in ANNEX 5.

Assessment criteria

Enhanced customer due diligence is conducted in prescribed circumstances. Enhanced due diligence is applied to 1) politically exposed persons 2) in non-face-to-face client identification situations 3) in the absence of originator information 4) where new technologies that provide anonymity are used and 5) in higher ML/TF risk situations.

5.5.2 Simplified customer due diligence

Reporting entities should conduct simplified customer due diligence in a manner and cases prescribed by the Act.

The reporting entity may conduct a simplified customer due diligence, at establishing the business relationship/conducting transactions, except in instances when there are reasons for suspicion of money laundering or terrorist financing in relation to a customer or a transaction, if the customer is a:

- **Financial institution -** bank, savings bank, post office, investment fund management company, pension company, securities trading company, insurance company of the AMLCFT Law or other equivalent institutions under the condition that such an institution shall be seated in a member-state or a third country;
- **State body -** state bodies, local and regional self-government bodies, public agencies, public funds, public, institutes or chambers;
- **Publicly traded company -** companies whose securities have been accepted and traded

on the stock exchanges or the arranged public market in one or several member-states in line with the provisions in force in the European Union, i.e. companies seated in a third country whose securities have been accepted and traded on the stock exchanges or the arranged public market in a member-country or a third country, under the condition that the third country have the disclosure requirements in effect in line with the legal regulations in the European Union area;

- **Low risk individual -** persons referred to in Article 7, paragraph 5 of AMLCFT Law for which a negligible money laundering or terrorist financing risk shall exist.

Simplified due diligence means that reporting entities must obtain the following data but are not required to conduct other customer due diligence measures such as identifying the beneficial owner:

1. when establishing a business relationship:
- name, address, seat and business registration number of the legal person establishing the business relationship, i.e. the legal person on whose behalf the business relationship is being established;
- name and surname of the legal representative or a person authorised by power of attorney who establishes business relationship on behalf of the legal person;
- purpose and intended nature of the business relationship and date of the relationship establishment;

2. when conducting transactions referred to in Article 9, paragraph 1, item 2 of this Law:
- name, address, seat and business registration number of the legal person for whom a transaction is being conducted;
- name and surname of the legal representative or a person authorised by power of attorney who conducts the transaction on behalf of the legal person;
- date and time of transaction execution;
- transaction amount and currency in which the transaction is being executed;
- manner of transaction execution;
- purpose of the transaction;
- name and seat of a legal person to whom the transaction is intended.

Note: A by-law has been issued by the Minister of Finance on June 18, 2009 which prescribes conditions for simplified due diligence. Reporting entities should refer to the by-law to ensure that requirements are fully met.

Assessment criteria
Simplified measures are appropriately applied. Simplified due diligence may be applied in certain circumstances if the customer is a financial institution, a state body, a publicly-traded company or a low risk individual. If simplified due diligence is applied the information listed in Section 5.5.2 of these Guidelines is collected.

5.6 Limitations in doing business with customers

Reporting entities should not conduct cash transactions in the following circumstances:

- cash collections exceeding the amount of HRK 105,000 selling goods and rendering services;
- sales of real-estate;
- receiving loans; and
- selling negotiable securities or stakes.

Assessment criteria

Transactions above HRK 105,000 in cash are not conducted in prescribed circumstances. The limitation of receiving cash payments shall also be in effect in instances when the payment with the said transaction shall be conducted in several interrelated cash transactions jointly exceeding HRK 105,000.00, i.e. the value of EUR 15,000.00. The cash collection limitation shall pertain to all legal and natural persons who shall receive cash through the said transactions during the performance of their registered business activities. The collections exceeding the amounts mentioned above must be conducted via non-cash means through a bank account, unless provided for otherwise in another Act.

6. On-Going Monitoring and Reporting

6.1 List of indicators

Reporting entities are obliged to have produced a list of indicators for the detection of suspicious transactions and customers. In producing the list, reporting entities should take into account their particular circumstances and the particular characteristics of the suspicious transaction.

Reporting entities must also use the list of indicators which must be an integral part of their internal enactment, as basic guidelines for determining their reasons for suspicion of money laundering and terrorist financing. The list of indicators must be maintained and updated in accordance with the money laundering trends and typologies known to them, as well as with circumstances stemming from their own operations.

Assessment criteria

A list of indicators is developed. Reporting entities should produce in a cooperation with competent bodies, a list of indicators for the detection of suspicious transactions and customers in relation to which reasons for suspicion of money laundering and terrorist financing shall exist (pursuant to Art 41 of the Act).

List of indicators should be included in internal enactment. The list of indicators referred shall be an integral part of the reporting entity's internal enactments.

List of indicators are updated annually. Reporting entities shall be obliged to upgrade and adapt the list in accordance with the money laundering trends and typologies known to them, as well as with circumstances stemming from the operations of the given reporting entity.

Note: The Minister of Finance may issue a special bylaw to prescribe mandatory inclusion of individual indicators into the list of indicators for the detection of suspicious transactions and customers in relation to which reasons for suspicion of money laundering or terrorist financing shall exist. No rule book has been issued as of the publication of this Guideline.

6.2 Measures of the business relationship monitoring

The reporting entity shall exercise due care in monitoring business activity performed by the customer, thereby ensuring knowledge of the customer's business, source of funds, intended nature and purpose of the business relationship, the customer's operations or transactions. On-going monitoring is not required when no business relationship has been established. This can be the case with respect to foreign exchange, real estate, dealers in precious metals and stones, auctioneers, pawn shops. However, reporting entities in all sectors are expected to conduct on-going monitoring when transactions of HRK 105,000 are conducted.

With respect to legal persons, the reporting entity must also carry out annual customer due diligence at least once a year, and no later than after the expiration of one year since the last customer due diligence had been conducted. With respect to individuals, the reporting entity must monitor the

business activity based on the reporting entity's assessment of the risk for money laundering or terrorist financing risk attached to these individual business undertakings.

Annual customer due diligence is also required for customers who are legal persons conducting transactions over HRK 105,000 when the legal person is seated in the Republic of Croatia and with 25% and greater ownership stake held by:

1. a foreign legal person which does not perform or is not allowed to perform trading, production or other activities in the domicile country of registration;
2. a trust or other similar foreign law company with unknown, i.e. hidden owners, secret investors or managers.

Exception
The repeated annual foreign legal person due diligence shall not be required if the foreign legal person is an obliged person referred to in Article 35, paragraph 1 of the Act.

Reporting entity is also required to keep the information up-to-date.for established business relationships. If the reporting entity does not have business relationships it does not have to keep information up to date

Assessment criteria

Business relationships and transactions of HRK 105,000 are monitored.
On-going monitoring is conducted in a risk sensitive basis with higher risk situation clients monitored more frequently.

Information is kept up to date for on-going business relationships. Documents and data available to the reporting entity must be kept up-to-date, and measures to be adjusted to the money laundering or terrorist financing risk level.

Annual due diligence of foreign persons is performed. Reporting entities shall regularly, at least once a year, and no later than after the expiration of one year since the last customer due diligence of the customer, conduct annual due diligence of foreign legal persons. In addition, annual customer due diligence should be performed on legal persons seated in the Republic of Croatia with 25% and greater ownership of a foreign legal person which does not perform or is not allowed to perform trading, production or other activities in the domicile country of registration; a trust or other similar foreign law company with unknown, i.e. hidden owners, secret investors or managers.

6.3 Complex and unusual transactions

Reporting entities must pay a special attention to all complex and unusually large transactions, as well as to each unusual form of transactions without an apparent economic or visible lawful purpose even in instances when reasons for suspicion of money laundering or terrorist financing have not yet been detected in relation to such transactions.

Reporting entities must also analyze the background and purpose of such transactions, and make a written record of the results of the analysis. These are to be made be available upon request to the AMLO and other supervisory bodies. Reporting entities must nonetheless report all suspicious transactions.

Complex and usual transactions are identified. Reporting entities should pay special attention to all complex and unusually large transactions, as well as to each unusual form of transaction without apparent economic or visible lawful purpose even in instances when reasons for suspicion of money laundering or terrorist financing have not yet been detected in relation to such transactions.

Analysis of background and purpose of transaction is documented. Also, reporting entities should analyze the background and purpose of complex and unusually large transactions, and make a written record of the result of the analysis.

Analysis of background and purpose of transaction is made available to the AMLO and other supervisory bodies. The reporting entity is also required to make the analysis available to the AMLO and other supervisory bodies upon request.

6.4 Reporting transactions to the AMLO

Reporting entities must report to the AMLO every transaction being conducted in cash totaling HRK 200,000.00 and more immediately, and no later than within three days upon the execution of the transaction. The CTR Form contains data prescribed with the Bylaw.

Exemptions for professionals on cash transactions: Persons involved in the performance of professional activities shall not be obliged to report to the AMLO on cash transactions referred except in instances when reasons for suspicion of money laundering or terrorist financing shall exist in relation with a transaction or a customer.

The Reporting entity shall be obliged to notify the FIU of suspicious transactions without any undue delay *before the transaction execution*, and to indicate in the report the reasons for suspicion of money laundering or terrorist financing, as well as the deadline within which the transaction is to be conducted.

Exceptionally, if the reporting entity was not in position to notify the FIU of the suspicious transaction before its execution in prescribed instances due to the nature of the transaction or due to the fact that the transaction was not executed or for other justified reasons, the reporting entity shall be obliged to report the FIU subsequently, and no later than the next business day. The suspicious transaction report is to substantiate the reasons for which the reporting entity was objectively unable to comply with what was prescribed.

Suspicious transaction reports should be supplied to the AMLO before conducting a transaction by phone, fax or in other adequate manner, and after conducting a transaction in the manner that is prescribed by the Minister of Finance in a bylaw.

Note: It should be noted that tax evasion is a criminal offence and a predicate offence to money laundering. In other words, if there is an attempt to conceal the proceeds of tax evasion this should be considered money laundering and should be reported to the Anti-Money Laundering Office.

Assessment criteria

CTR Cash transaction reports are reported in the prescribed manner within 3 days. Every cash transaction over HRK 200,000 and more must be reported to the AMLO immediately and no later than 3 days after the completion of the transaction using the CTR Form.

STR Suspicious Transaction Reports are reported without any delay in the prescribed manner. The Reporting entity shall be obliged to notify the FIU of suspicious transactions without any undue delay *before the transaction execution*, and to indicate in the report the reasons for suspicion of money laundering or terrorist financing, as well as the deadline within which the transaction is to be conducted.

Reporting entity refrains from conducting a suspicious transaction. The Reporting entity is obliged to refrain from conducting a transaction for which the reporting entity shall know or suspect to be connected with money laundering, i.e. terrorist financing**.**

6.5 Reporting from persons performing professional activities about suspicious transactions and persons

Professionals are required to report suspicious transactions when they engage in activities listed in Section 2.4.2 of these Guidelines. Suspicious transaction reporting shall not apply to the persons involved in the performance of professional activities in respect of information they receive from or obtain on a customer during the course of establishing the legal position of the customer or during the representation of the customer in relation with a court proceeding which shall include advice on proposing or avoiding court proceeding, whether such information is received or obtained before, during or after the completion of such court proceedings.

Assessment criteria

Professionals report suspicious transactions immediately and in the prescribed manner. Lawyers, law firms and a notaries public, as well as auditing firms and independent auditors, legal and natural persons involved in the performance of accounting services and tax advisory service, when engaged in triggering activities, report suspicions of money laundering or terrorist financing undertake to notify the AMLO without any undue delay in the prescribed manner.

Professionals inform AMLO within three days when client seeks advice on money laundering or terrorist financing. In all instances when the customer seeks an advice from persons involved in the performance of professional activities on money laundering or terrorist financing, the persons involved in the performance of professional activities shall undertake to immediately notify the FIU thereof, and no later than within three business days from the date the customer sought for such an advice.

7. DATA KEEPING AND RECORD KEEPING

7.1 Data Keeping

Reporting entities must to keep data collected on the basis of this Law and regulations a period of ten years after the execution of a transaction execution or the termination of a business relationship. Data and accompanying documentation on an authorised person and the authorised person's deputy, the professional training of employees and the performance of internal audit must be kept for a period of four years after the appointment of the authorised person and the authorised person's deputy, the delivery of professional training or the performed internal audit.

Exception for professionals. Lawyers, law firms and notaries public, auditing firms and independent auditors, legal and natural persons involved in the performance of accounting services and tax advisory services must keep the data and the accompanying documentation they collected for a period of ten years after the completion of customer identification. They must also keep data and the accompanying documentation on professional training of employees for a period of four years after the delivery of the training.

Assessment criteria

Documents are kept for 10 years from the date of transaction or the end of the business relationship. Reporting entities must keep data collected on the basis of the Act and regulations passed on the basis of the Act and the accompanying documentation for the period of ten years after a transaction execution or the termination of a business relationship.

Data on the authorized person, training, internal audit is kept for four years. The reporting entity shall undertake to keep data and the accompanying documentation on the reporting entity's authorized person and the authorized person's deputy, the professional training of employees and the performance of internal audit for the period of four years after the appointment of the authorized

person and the authorized person's deputy, the delivery of professional training or the performed internal control.

7.2 Record keeping

Reporting entities must keep the records on customers, business relationships and transactions referred to in Article 9 of the Act and records on the supplied data referred to in Articles 40 and 42 of the Act. Reporting entities should maintain the following records:

- Data about the conducted transactions amounting to HRK105,000 or more;
- Data about the linked transactions reaching the total amount of HRK105,000 or more;
- Data about the other suspicious transactions established in accordance with the list of indicators;
- Data regarding complex and unusually large transactions, as well as transactions of unusual form even in instances when the reasons for suspicion on money laundering or terrorist financing have not yet been detected, according to the Article. 43 of AMLCFT Act;
- Data on clients and transactions for transactions of selling/buying foreign currency- submitted to AML Office (larger than HRK105 000, linked transactions and suspicious transactions);
- Records on examinations conducted by supervisory bodies which include: name of the supervisory body, name and surname of the authorized officer who conducted the examination, date and time of examining data, information and documentation.

Professionals are obliged to keep the following records in chronological order.

- The records on data on clients, business relationships and transactions linked with the implementation of client due diligence measures,
- The records on data that are submitted to the Office according to Article 54, paragraph 1 and 2 of the Act, and that refer to suspicious transactions and persons, as well as asking for advice in connection with money laundering and terrorist financing,
- The records on the checks performed by the Financial Inspectorate and/or the Office of data, information and documentation, comprising, besides the name of a supervisory body, first and last name of the authorized official person who has performed the checking, date and time of data checking.
- The records on clients, business relationships and reported suspicious transactions according to Article 4 of the Ordinance contains the following data: client's first and last name, type and date of the establishment of a business relationship, date of implementation or of rejection of the execution of a transaction, date of asking for advice in relation to money laundering or terrorist financing and date of reporting to the Office.

Assessment criteria

- **Records are kept according to the legislative requirements.** Reporting entities are required to keep records on customers, business relationships and transactions referred to customer due diligence and cash transactions and suspicious transactions and persons reports.

Note: A by-law on record keeping has been issued by the Minister of Finance with respect to professionals. Professionals should consult the bylaw for specific requirements.

Examination records are kept. All reporting entities shall keep records on examinations conducted by supervisory bodies of data, information and documentation which include: name of the supervisory body, name and surname of the authorized officer who conducted the examination, date and time of data examination.

8. AML/CFT requirements are applied in majority-owned subsidiaries

As previously noted in Section 2.4.1.1 of these Guidelines, the Act prescribes in Article 5 an obligation for reporting entities that have business units and companies seated in third countries with majority ownership or with predominant decision-making rights exercised by the reporting entities to ensure that money laundering and terrorist financing prevention and detection measures are applied within the equal scope in their business units and companies, unless such a course of action would be in direct contradiction to the legal regulations of the third country. Where the legislation of the third country does not permit the application of the money laundering and terrorist financing prevention and detection measures within the scope prescribed by this Act, reporting entities must inform the AMLO of the matter without any undue delay and to institute adequate measures for the elimination of the money laundering or terrorist financing risk.

Reporting entities must regularly inform their business units and companies in their majority ownership or in which they shall have predominant decision-making rights, seated in a third country, of internal procedures pertinent to money laundering and terrorist financing prevention and detection, especially in terms of customer due diligence, supply of data and information, keeping records, internal control and other significant circumstance related with the money laundering and terrorist financing prevention and detection.

Assessment criteria

Internal procedures are communicated to majority-owned subsidiaries. To be effective in meeting this requirement reporting entities must ensure that the money laundering and terrorist financing prevention and detection measures are applied with equal scope in their business units and majority-owned subsidiaries, seated in a third country and that they regularly inform their business units and majority-owned subsidiaries seated in a third country on internal procedures pertinent to money laundering and terrorist financing prevention and detection.

Reporting entity communicates to FIU if subsidiary is located in country where the Act's obligations cannot be extended. Where the legislation of the third country does not permit the application of the money laundering and terrorist financing prevention and detection measures within the scope prescribed by the Act, the reporting entity shall be obliged to inform the FIU about it, without any undue delay and to institute adequate measures for the elimination of the money laundering or terrorist financing risk.

9. IT System

Credit institutions must establish an adequate information system relevant for their respective organisational structures in order to be able to promptly, timely and completely provide the AMLO with data.

Assessment criteria

Information system is established for credit institutions. Reporting entities should ensure that credit institutions have established an adequate information system due to their respective organizational structures in order to be able to supply the FIU rapidly, timely and completely with data as to whether or not they shall maintain or have maintained a business relationship with a given natural or legal person, as well as to the nature of such a relationship.

Information system ensures that CDD information is easily retrievable. The information system should allow customer due diligence and transaction information to be easily retrievable.

Information system allows for monitoring of transactions. Also, reporting entities should ensure that the compliance officer has partaken in the establishment and development of IT support for carrying out activities in the field of money laundering and terrorist financing prevention and detection within the reporting entity and whether the reporting entity ensured adequate IT support

enabling ongoing and safe monitoring of the activities in the field of money laundering and terrorist financing prevention and detection.

10.What to expect from the Financial Inspectorate

10.1 What you can expect from the Financial Inspectorate staff

10.1.1 Professionalism

The Financial Inspectorate's approach to ensuring compliance is cooperative. Reporting entities should expect to be treated professionally and courteously. Staff of the Financial Inspectorate is held to high standards as they are required by the Financial Inspectorate Act to comply with the law and the code of Ethics for Government employees.

10.1.2 Protection of your information

Personal, transactional and financial information will be protected against unauthorized use or disclosure. The Financial Inspectorate Act creates a mandatory expectation of the protection and use of secret and classified data which would have been obtained during the course of exercising the supervisory role. The Financial Inspectorate is only permitted to use data for the performance of its work, in minor proceedings or in proceedings before a court.

10. 3 Information and assistance

Authorized persons strive to explain clearly and consistently the policy interpretations and to facilitate your understanding of the legislative obligations, as well as of the Financial Inspectorate's Guidelines, policies, and procedures. In addition, the Financial Inspectorate will work with other supervisory bodies to assist reporting entities by publishing a list of indicators. Should you require information or assistance, do not hesitate to contact the Financial Inspectorate at the following address:

Insert address and telephone and email coordinates

10.4 Requests for information from the Financial Inspectorate

A proper compliance regime allows the Anti-Money Laundering Office to receive the quantity and quality of reports it requires to produce solid financial intelligence and assures law enforcement and security agencies of quick access to information because of improved client identification and record keeping practices. In other words, by creating compliance regimes that conform to the law, reporting entities become part of a larger effort to combat money laundering and terrorist activity financing.

In making sure that reporting entities comply with their obligations, the Financial Inspectorate takes a co-operative approach. While exercising its authority to examine compliance, the Financial Inspectorate is committed to working with reporting entities in a partnership that enhances the integrity of Croatia's financial systems and promoting greater public safety.

Normally, a Financial Inspectorate authorized person (person who will carry out the examination for anti-money laundering and anti-terrorist financing purposes from the Financial Inspectorate) will provide advance notice of the examination, which would be scheduled by telephone and confirmed in a letter to the reporting that will be examined. Prior to arriving, the authorized person may request documentation including your internal enactment, your policies and procedures, the annual review, of your policies and procedures, samples of transaction documentation, as well as other documents. This will allow a portion of the examination to begin before arriving on-site and thus limit the amount of time our authorized persons are in your place of business.

10.5 During On-site examinations

As noted previously, you will be provided advance notice of an on-site examination. In exceptional circumstances, no advance notice will be given. The Financial Inspectorate Act gives the Financial Inspectorate the power to enter a business to carry out an on-site examination without prior notice.

At the conclusion of the examination, the authorized person will provide a review of the finding verbally. A letter outlining any deficiencies will be provided by the Financial Inspectorate, following the on-site examination. Reporting entities will also be asked for an action plan and timelines to remedy any deficiencies.

What will be examined?

An anti-money laundering and anti-terrorist financing examination by the Financial Inspectorate will try to determine if the entity is meeting its obligations under the legislation. The **Assessment Criteria** listed in these Guidelines provide a useful list of the areas that may be examined by authorized officers. The provision of these Assessment Criteria to reporting entities promotes collaboration, transparency and eliminates surprises for reporting entities in terms of the areas that may be examined by an authorized person. This is effective and efficient for both reporting entities and the financial Inspectorate. It is also a useful tool for reporting entities in testing the strength of their own policies and procedures during their annual review. Summarily, some areas of examination can include:

- Adoption of an internal enactment;
- Appointment of a compliance officer with proper authority and role;
- Presence and update of an indicators list;
- Implementation of a risk-based approach;
- Implementation of policies and procedures;
- Review of the presence of a review process of the policies and procedures;
- Development and implementation of a training program;
- Reporting of all required transactions;
- Implementation of client identification and record keeping requirements;

These Guidelines will help reporting entities prepare for an examination by the Financial Inspectorate.

10.6 Sanctions for non-compliance

While most reporting entities will endeavour to comply with the anti-money laundering and legislation and regulations, invariably some will have deficiencies and some will not comply fully. The Act provides for penalties to be applied for non-compliance. Penalties may range from HRK 25,000.00 to HRK 700,000.00. To better understand the range of potential infraction and penalties, please consult the Act or contact the Financial Inspectorate.

ANNEX 1 – BASIC LIST OF INDICATORS

The basic list of indicators for recognizing suspicious transactions and clients, which attorneys at law and public notaries are obliged to update:

General indicators

-a client says or admits being involved in criminal acts,
-a client does not want their mail to be addressed to a location in a country,
-a client has accounts in several financial institutions at the same territory without the right reason,
-a client has been followed or monitored,
-a client shows great interest in the system of organizing and in controls and policy of their implementation,
-a client is not known and opposes personal contact meeting,
-a client's private or official telephone number is off or does not exist,
-a client has been involved in businesses which are not characteristic of their doing business,
-a client, without any special reason, encourages the fast performance of business or transaction,
-a client has recently established more business relationships with different financial institutions,
-a client tries to establish good and close relationships with personnel,
-a client uses different names or nicknames and a whole series of similar, but different addresses,
-a client uses addresses of post boxes or other types of postal addresses instead of an address of a street, which is not common for the mentioned place or area,
-a client offers money, gifts, or other unusual benefits as a counter favour for the execution of an evidently unusual or suspicious business deal,
-a client is under the investigation for the criminal act of money laundering or financing of terrorism,
-a client wants to assure an employee to fail to complete a document necessary for the execution of a business deal or a transaction,
-a client's acting in relation to the request on a notification demonstrates their desire to avoid the fulfilment of this duty,
-a client is very well familiar with the rules of notification on suspicious transactions,
-a client if very well familiar with cases relating to money laundering or terrorist financing,
-a client begins to conclude very quickly by themselves that funds are "clean" and not "laundered".

Identification documents

-a client provides suspicious or unclear information,
-a client submits inadequate documents for checking; they are forged, altered or incorrect,
-a client is against the submission of identity documents,
-a client submits only copies of identity documents,
-a client tries to perform identification with other documents not being those proving identity,
-a client is too late with the submission of company documents,
-all identity documents are issued abroad, and their authenticity is hard to verify,
-all enclosed identity documents seem new or issued very recently.

Cash transactions

-a client wants to do business in cash, although it is not a common way for their profession,
-a client brings larger amounts of money which has not been counted,
-a client wants an attorney at law or a public notary to keep and on their behalf deposit/pay larger amounts of money.

Economic reasons

-a business relationship is not in line with client's financial condition or usual doing business,

-a business relationship or a transaction is not in accordance with the usual way of performing activities, i.e. they do not have economic value for a client,
-a business relationship or a transaction is unnecessarily getting complicated,
-a client's activities are not in accordance with expectations in relation to the performance of an activity,
-a business relationship or a transaction also involves (as incidental members) non-profit or charity organizations, without a justifiable economic reason.

Business relationship or transaction involving other countries

-clients and other parties included in a business relationship do not have visible or reasonable business or other links with Croatia,
-a client uses means of payment, issued in another country, although they do not perform an activity in that country or do not have permanent nor habitual residence in it,
-a business relationship or a transaction involves countries known for banking or economic system allowing the individuals or companies a high degree of confidentiality or concealed activity.

Business relationship or transaction linked with tax oases (offshore)

-accumulation of larger amounts, which are not in line with the scope of client's business activity, that have been transferred to tax oases,
-loans with guarantees of banks from tax oases,
-using means of payment issued by banks from tax oases.

ANNEX 2 - SPECIFIC INDICATORS FOR ATTORNEYS AT LAW AND PUBLIC NOTARIES' PROFESSION

-a client's doing business greatly differs from the usual doing business of this profession,
-a client lives beyond their real possibilities,
-a client receives payments from unknown sources,
-a client does not employ any personnel which is not common for their doing business,
-a client continuously does business with loss for which there are not any justifiable reasons,
-a client requests a service of performing a financial transaction which is different from usual business activities or it can be performed more favourably in some other way, and so a client alludes to the protection of data and to evident avoidance of the determination and checking of identity which is common within financial institutions,
-a client requests from attorneys at law and public notaries the performance of a financial transaction and the avoidance of the usual payments system, acting very unusually and nervously,
-a client is accompanied by third persons not being obviously linked with the request for a transaction,
-a client asks questions about registering a company in the court register in a way which is not usual for regular registering procedures, and without evident economic-business purpose,
-a client asks for an advice from an attorney at law or a public notary on unusual transactions or services for the purpose of obvious concealment of illegal origin of funds,
-a client appears at attorney at law or public notary with a larger amount of cash, gold, precious stones or securities or other liquid monetary instruments trying to deposit them or transmit them for the performance of a certain transaction or a business relationship, and in a way unusual for regular financial operations or with visible endeavour to circumvent financial institutions,
-a client concludes or attests contracts which are unusual and the economic-business background does not justify this way of contracting,
-a client asks for attorneys at law and public notaries' services in unusual business hours (early in the morning, late at night, outside business hours) or asks for a quick execution without justified reasons,
-transactions and other business services, as ordered by a public person, which differ from the usual ones, and without evident logical economic purpose,
-a client asks questions about unusual ways of paying in business operations linked with real estates,
-clients do not want to identify themselves in case of a one-off transaction or linked financial transactions of more than HRK 105,000.00 or identify themselves with forged data and identity documents,
-a client being a natural or a legal person asks questions on or performs transactions with real estates for natural and legal persons, residents and non-residents who/which come from offshore destinations or for offshore companies,
-a selling price of a real estate determined by a client is not in accordance with prices of real estates on the market,
-a client disposes of a comprehensive personal and consumable property (vessels, luxury cars, apartments for living and residences) which does not take part in the usual framework of a company or profession's doing business,
-invoices are made to a client for provided services of a company or an organization having headquarters in countries that do not have the appropriate legislation for money laundering prevention, and which are known as tax oases, i.e. the ones with the banking system allowing anonymity to clients.

ANNEX 3 – HIGH RISK SITUATIONS

High Risk Situations Related To Customer Risk May Include:

- politically exposed persons,
- foreign legal persons that do not perform nor are allowed to perform trading activity in the country they have been registered in trusts,
- charitable or other non-profit organizations, which do not have an organized supervision of its doing business by competent supervisory bodies or structural supervision bodies (particularly those that often work cross-border),
- clients with complex organizational structure or nature which disables the determination of a beneficial owner, that is, unexplainable use of legal persons or legal arrangements, endorsements,
- clients that establish their business relationships, that is, perform transactions in unusual circumstances, for example:
    - significant and unexplainable geographic distance between the headquarters of the customer and the reporting entity, and
    - frequent and illogical changing of business partners for the performance of the same jobs
- clients with complex organizational structure or nature which disables the determination of a beneficial owner,
- clients with a beneficial owner towards who the compulsive measures have been carried out due to the establishment of international peace and safety in accordance with the UN Safety Council resolutions,
- clients for which there is a doubt that they not act for their account,
- clients for which there are indications that they perform suspicious transactions,
- clients with intensive cash operations,
    - clients dealing with money operations
    - casinos and other organizers of games of chance, betting houses and
    - clients whose activity is not cash-intensive, but some transactions are performed by using larger cash amounts,
- clients establishing a business relationship through an accountant or tax adviser or a person carrying out an activity on the client's behalf,
- clients using financial intermediaries, financial institutions or lawyers and public notaries who are not subjects to the application of measures for preventing money laundering and financing of terrorism and are not adequately supervised by competent bodies or professional associations (chambers),
- clients being accused of an offence by which a property has been obtained (illegally acquired property),
- clients who do not have an address or who have several addresses without justified reason,
- clients changing an enforcement order without relevant explanation,
- using legal persons and subjects equalized with them without visible legal, legislative, business, economic reason etc.
- persons appearing on the terrorist or criminal list
- international clients from high risk jurisdictions
- clients engaged in quasi legal activities, such as internet gaming
- intermediaries, such as lawyers and accountants
- intermediary structures, such as holding companies, legal arrangements numbered companies that have no apparent business purpose
- clients whose geographic distance from the reporting entity is not explainable
- clients whose nature, structure or relationship make it difficult to identify the ultimate beneficial owner
- clients whose nationality/residence/location of employment is associated with a country on a prohibited country list or a high risk country list

- cash and cash equivalent intensive businesses, such as: casinos, MSBs, foreign exchange business, etc.

High Risk Situations Related To Products and Services Risk
May Include:

- participating or assisting in the establishment of a company,
- lending addresses to foreign legal persons,
- performing tasks for the purpose of concealing the client's beneficial owner,
- performing tasks of real estate transfer between clients in unusually short time period without visible legal, economic or other justified reason,
- performing tasks linked with an inheritance of a person known to an attorney at law or a public notary for convictions for offences connected with illegal acquisition of property,
- services within which the reporting entity acts as financial intermediaries and actually perform the receipt and transfer of funds through accounts they actually control by performing a business transaction,
- providing services linked with establishing, operating or managing of a shell company, company in nominal ownership,
- services which deliberately offer more anonymity or depend on more anonymity of a client or participants than it is usual considering the circumstances and an attorney at law or a public notary's earlier experience,
- services of illegal concealing of beneficial ownership from competent bodies,
- transfer of ownership over real estates between clients in a time period which is unusually short for similar transactions without obvious legal, tax, business or any other justified reason.
- payment of financial funds on the account of a client or payment on the account of a client which is different from the account mentioned during the identification through which they usually operate,
- transactions intended for persons with a domicile or headquarters in a country which is known as a financial or tax oasis (offshore financial centre),
- transactions intended for non-profit organizations having headquarters in a country known as an offshore financial centre, financial oasis or neither a member of the European Union nor a signatory of the Agreement on the European Economic Area.

High Risk Situations Related To Business Relationship/Delivery Channels
Risk May Include:

<u>Business relationships</u>

- business relationships involving complicated financial transactions,
- business relationships involving transactions linked with real estates,
- business relationships involving payments towards/from third persons and cross-border payments,
- business relationships involving cash payments,
- business relationships involving products which are at higher risk for money laundering and financing of terrorism: all transferable instruments which are made out to the bearer, as well as transferable instruments issued on the bearer or in favour of a fictitious receiver, endorsed without forbiddances or in other forms allowing the transfer of title through transmission or some other incomplete instruments which are signed, but without mentioning the name of a payment beneficiary,
- payments received from unconnected or unknown third parties and payments of fees in cash when this is not a common way of paying.
- clients who offer payment of unusual fees for the services which, as a rule, do not justify such a fee. However, agreements on the appropriate fee for unpredictable circumstances, when a significant reward can be received for a successful representation, should not necessarily be considered as a risk factor, and

- a client asks for services which are not within the scope of an attorney at law or a public notary's professional activity.

Delivery Channels

- ddeposit taking, especially cash, and insurance products that allow large one-time or regular payments or deposits, to be made and subsequently withdrawn,
- credit accounts where large credit balances are allowed to be maintained,
- wire transfers,
- trade finance services,
- private banking,
- "free look" or "cooling off" periods coupled with premium refunds,
- payable through accounts,
- internet banking,
- sale of stored value cards,
- supports high transaction volumes, high speed movement of funds,
- use of intermediaries or introducers e.g. Mortgage and deposit agents, and
- internet, telephone and mail as a substitute for face to face interaction

High Risk Situations Related To Geographical Risk May Include:

- a country which is not a member of the European Union nor a signatory of the Agreement on the European Economic Area,
- a country against which the United Nations or other international institutions have imposed sanctions, embargo or other similar measures,
- a country which is known, based on the knowledge of relevant international organizations, for a high degree of organized criminal, particularly corruption, arms trade, trafficking in human beings or for breaching human rights, production or organized and developed drug trade,
- a country which, according to the data of the international organization FATF, appertains to non-cooperative countries or territories or if it is about an offshore financial centre,
- countries which are estimated by relevant international organizations as countries lacking the appropriate AML/CFT legislation, regulations and other measures,
- countries in which the undertaking of terrorist activities is being supported or enabled,
- a country which an attorney at law or a public notary considers risky based on their own judgment,
- a country subject to Croatian or other national sanctions, embargoes or similar measures,
- a jurisdiction subject to United Nations Security Council sanctions,
- a jurisdiction identified by credible sources as providing support for terrorist activities,
- a jurisdiction identified by credible sources as having significant levels of corruption or other criminal activity,
- a jurisdiction not member of the FATF, and
- regional or local geographical factors related to risk (e.g., Croatian domestic risk based on urban vs. rural; known crime/gang areas, etc.)

ANNEX 4 - RISK ASSESSMENT CHECKLIST

The following checklist is intended to provide an example of how to assess risk for your clients, products, services, delivery channels and geographic locations. This is only a starting point and you should customize the checklist for your business. If you already use another risk assessment tool, you can continue to use it or enhance it as necessary.

If you answer *yes* to any of the questions below, you should consider it as higher risk for money laundering or terrorist financing. Risk-mitigation steps should be taken where appropriate. See subsection 4.1.2 for more information.

	YES	**NO**	**N/A**
Customer Risk			
Do you have clients that:			
• operate in a cash intensive business?			
• reside outside Croatia?			
• are intermediaries or "gatekeepers" such as professionals that hold accounts for clients where the identity of the underlying client is not disclosed to you?			
• are an unregistered charity or other unregulated “not for profit” organisation (especially one operating on a “cross-border” basis)?			
• are located in a known high crime rate area?			
• offer on-line gaming?			
• the nature of their business makes it difficult to identify the true owners or controllers?			
• are foreign politically exposed persons?			
• do not have an address or who have several addresses without justified reason?			
• have a criminal record?			
• have links to organized crime?			
Product/Service Risk			
Do you offer products or services that:			
• make it difficult to fully identify clients?			
• assist in the establishment of a company?			
• lend addresses to foreign legal persons?			
	YES	**NO**	**N/A**

Do you:			
• perform tasks for the purpose of concealing the client's beneficial owner?			
• perform tasks of real estate transfer between clients in an unusually short time period without visible legal, economic or other justified reason?			
• provide services linked with establishing, operating or managing of a shell company, company in nominal ownership?			
Delivery Channels/Business Relationships Risk			
Do you:			
• conduct non-face-to-face transactions?			
Do you have business relationships that:			
• involve complicated financial transactions?			
• involve payments towards/from third persons and cross-border payments?			
• involve high risk real estate transactions?			
• involve cash payments?			
Geographical Risk			
Do you or your clients operate or undertake activities in the following countries:			
• Any country which is neither a member of the European Union nor a signatory of the Agreement on the European Economic Area?			
• Any country subject to sanctions, embargoes or similar measures issued by the United Nations (UN)?			
• Any country identified as a financial secrecy haven or jurisdiction?			
• Any country identified by the Financial Action Task Force (FATF) as non-cooperative in the fight against money laundering or terrorist financing or subject to a FATF statement?			
• Any country identified by credible sources as lacking appropriate money laundering or terrorist financing laws and regulations or as providing funding or support for terrorist activities?			
• Any country that is known to have significant levels of corruption, or other criminal activity?			

ANNEX 5 - RISK MITIGATION MEASURES

MITIGATION MEASURES FOR HIGH RISK SITUATIONS

- increased awareness of higher risk situations within business lines across the entity;
- increased monitoring of transactions;
- the approval of the establishment of relationships is escalated to senior management;
- the levels of on-going controls and reviews of relationships are increased;
- personnel that have clear lines of authority, responsibility and accountability;
- adequate segregation of duties (for example, an employee establishing a relationship with a client is not authorized to also approve it as that authorization is the responsibility of someone else in the organization);
- proper procedures for authorization (for example, an employee processing a transaction for which the amount exceeds a certain threshold has to follow a procedure to get approval for the transaction by someone else in the organization); and
- internal reviews to validate the risk assessment processes.
- seeking additional information beyond the minimum requirements to substantiate the client's identity or the beneficial ownership of an entity;
- obtaining additional information about the intended nature of the relationship, including estimates regarding the amount and type of business activity;
- obtaining additional documented information regarding the client' source of funds and accumulation of wealth;
- requesting high risk clients to provide additional, documented information regarding controls they have implemented to safeguard their operations from abuse by money launderers and terrorists;
- getting independent verification of information (i.e. from a credible source other than the client);
- stopping any transaction with a potential client until identification information has been obtained;
- implementing an appropriate process to approve all relationships identified as high risk as part of the client acceptance process or declining to do business with potential clients because they exceed your risk tolerance level;
- implementing a process to exit from an existing high risk relationship which is beyond the entity's stated risk tolerance level; and
- analyzing money laundering and terrorist financing risk vulnerabilities for new acquisition processes and for product or service development processes.

ANNEX XXIX HANFA: Guidelines for the implementation of the Anti-Money Laundering and Terrorist Financing Act for the reporting entities falling within the competence of the Croatian Financial Services Supervisory Agency

I PURPOSE

Pursuant to Article 88 of the Anti-Money Laundering and Terrorist Financing Act (Official Gazette 87/08, hereinafter: the Act), the Croatian Financial Services Supervisory Agency (hereinafter: the Agency) is authorised to issue independently or in conjunction with other supervisory bodies guidelines for the implementation of individual provisions contained in the Act and regulations adopted on the basis thereof. The Guidelines for the prevention of money laundering and terrorist financing (hereinafter: the Guidelines) were adopted with a view to ensuring uniform implementation of the provisions of the Act and regulations adopted on the basis thereof by:

1 investment fund management companies, business units of third country[8] investment fund management companies, investment fund management companies from Member States which have a business unit in the Republic of Croatia, i.e. which are authorised to directly perform fund management business in the territory of the Republic of Croatia and third parties which are allowed, in keeping with the law regulating fund operations, to be entrusted with certain matters by the respective management company;

2 pension companies, including pension fund management companies and pension insurance companies;

3 companies authorised to do business with financial instruments and branches of foreign companies dealing with financial instruments in the Republic of Croatia;

4 insurance companies authorised for the performance of life insurance matters, branches of insurance companies from third countries authorised to perform life insurance matters and insurance companies from Member States which perform life insurance matters directly or via a branch in the Republic of Croatia;

5 legal and natural persons performing business in relation to factoring;

6 legal and natural persons performing business in relation to leasing;

7 insurance agents for entering into life insurance agreements; and

8 insurance intermediation for entering into life insurance agreements, (hereinafter: reporting entities).

[8] Third country is a non-EU Member State or a non-signatory state to the Agreement creating the European Economic Area.

II BASIC PRINCIPLES OF THE FIGHT AGAINST MONEY LAUNDERING AND TERRORIST FINANCING

1. Customer identification and verification

The reporting entities shall, before establishing a business relationship with a customer or before carrying out a transaction involving amounts exceeding the amount prescribed by the Act or in other cases envisaged by the Act, obtain the necessary information on the customer, so as to determine and verify their identity. Credible customer identification can be made only on the basis of valid, independent and objective sources, such as an official identification document, or other public document verifying the veracity of the customer's identity (official personal documents, notarised extract from the court or other public register). Where a customer's identity cannot be determined or verified, the reporting entity shall not enter into a business relationship or execute a transaction and shall terminate all the existing business relationships with such a customer.

2 Legislative compliance and compliance with standards

In carrying out their registered activity, the reporting entities shall behave in accordance with the adopted laws and subordinate legislation that regulate the area of detection and prevention of money laundering and terrorist financing and ensure that the prescribed measures are incorporated in their business activities on all levels in a manner that ensures full compliance of the reporting entities with the Act.

3 Cooperation with the Anti-Money Laundering Office and the Agency

Within the framework of their authorities under the law, the reporting entities shall ensure full cooperation with supervisory authorities such as the Agency and the Anti-Money Laundering Office (hereinafter: the Office). The obligation of cooperation between the reporting entities and supervisory bodies is especially important as regards the submission of documents and data and information that relate to customers or transactions which raise suspicion of money laundering or terrorist financing. The cooperation is also essential as regards reporting on any kind of behaviour or circumstances, that are, or might be connected to money laundering or terrorist financing and that might be prejudicial to the safety, stability and reputation of the financial system of the Republic of Croatia. It is exactly for that reason that the accepted internal procedures shall under no circumstances, directly or indirectly restrict the cooperation between the reporting entities and the Agency and/or the Office, or in any way affect the efficacy of such cooperation.

4 Adoption of internal policies, procedures and internal audit

The reporting entities shall adopt a uniform policy for the management of money laundering and terrorist financing risks, and adopt on the basis of that policy efficient internal procedures that are to cover in particular customer verification, risk analysis, and identification of customers and transactions which raise suspicion of money laundering or terrorist financing. It is essential to acquaint all employees with these procedures and to ensure full employee compliance with these procedures in the course of their work. The policy of the reporting entities, as regards risk management, shall cover customer reception and handling procedures, risk analysis preparation procedures, employee education processes, internal audit mechanisms, suspicious transactions detection and reporting procedures, and the responsibility of employees for the implementation of the measures for the detection and prevention of money laundering or terrorist financing.

5 Continuous employee education

The reporting entities shall ensure continuous professional training and education of all employees directly or indirectly involved in the performance of the tasks of prevention or detection of money laundering and terrorist financing or performance of tasks which involve a higher degree of risk in terms of money laundering or terrorist financing as well as of external staff and agents that the reporting entity has authorised to perform individual tasks on the basis of an agreement.

III RISK ASSESSMENT

1 Purpose of risk analysis

Under the Act, the risk of money laundering or terrorist financing means the risk of abuse, by the customer, of the financial system of the Republic of Croatia for money laundering or terrorist financing, i.e. the risk that a business relationship, transaction or product will be directly or indirectly used for money laundering or terrorist financing. To prevent excessive exposure to the negative effect of money laundering and terrorist financing, the reporting entity shall, in accordance with the Act, make a risk assessment. This assessment determines the level of exposure of an individual customer, business relationship, product or transaction to the risk of money laundering or terrorist financing. The preparation of risk analysis is a key precondition for the implementation of the prescribed customer due diligence measures. The risk category assigned to a customer, business relationship, product or transaction will determine the type of customer due diligence measure that the reporting entity is obligated to implement under the Act (regular customer due diligence, enhanced customer due diligence and simplified customer due diligence).

2 Risk management policy and risk analysis

The reporting entity, i.e. its management board, may, where this is necessary to ensure more efficient implementation of the provisions of the Act and the Guidelines, before preparing risk analysis, adopt an adequate policy for the management of money laundering and terrorist financing risks. The primary purpose of such a policy is to determine, on the level of reporting entities, those business areas that are more or less critical in respect of possible abuse relative to money laundering or terrorist financing, i.e. to enable the reporting entities to identify and determine on their own the key risks in these areas and define measures for dealing with those risks. In formulating the foundations for the adoption of money laundering or terrorist financing risk management policy, the reporting entity shall take into account the following criteria and define them in more detail in the formulation of its policy:

1 the purpose and the objective of money laundering and terrorist financing risk management and their correlation to the business objective and strategy of the reporting entity;

2 the areas and business processes of the reporting entity that are exposed to the risk of money laundering and terrorist financing;

3 the risks of money laundering and terrorist financing in all key business areas of the reporting entity;

4 the measures for dealing with the risk of money laundering and terrorist financing;

5 the role and the responsibility of the management board of the reporting entity in the introduction and adoption of money laundering and terrorist financing risks management.

3 Preparation of risk analysis

Risk analysis is the procedure whereby the reporting entity:

- provides an assessment of the probability of abuse of its business operations for money laundering or terrorist financing;
- defines the criteria on the basis of which an individual customer, business relationship, product or transaction is classified as more or less risky in terms of money laundering or terrorist financing;
- determines the consequences and defines the measures for efficient management of such risks.

In the preparation of risk analysis, the reporting entity shall take into account the following criteria:
1 the reporting entity shall base the risk category on the exposure criteria determined in chapter 3.5 of the Guidelines which are used during customer due diligence measures to classify a customer, business relationship, product or transaction into one of the risk categories in accordance with chapter 5.6 of the Guidelines;
2 in determining the risk category, the reporting entities may, based on the risk criteria determined in the Guidelines, and in accordance with their risk management policies, classify a

customer, business relationship, product or transaction as a high-risk category in terms of money laundering or terrorist financing and conduct a customer due diligence analysis;

3 in determining the risk category of a customer, business relationship, product or transaction that are pursuant to the Act and the Guidelines determined as high-risk categories, the reporting entity shall in no way classify such risk categories as being of medium (average) or negligible risk. Similarly, the reporting entity shall not act contrary to the provisions of the Act and subordinate legislation or Guidelines and expand on its own initiative the group of customers, business relationships, products or transactions that are to be treated as posing negligible risk.

4 Preparation of risk assessment

4.1 Initial risk determination

Based on the performed risk analysis, the reporting entity shall make a risk assessment of each individual customer, business relationship, product or transaction immediately before entering into a business relationship or executing a transaction and after it has performed the following:

1 determine the identicalness of the customer against the required collected data on the customer, business relationship, product or transaction and other data that the reporting entity is obligated to collect for the preparation of risk assessment;

2 evaluate the obtained data in terms of the criteria of risk of money laundering or terrorist financing (risk determination);

3 make a risk assessment of the customer, business relationship, product or transaction, based on the previous risk analysis, and classify the customer, business relationship, product or transaction into one of the risk categories;

4 conduct customer due diligence measures (regular, enhanced, simplified);

5 enter into a business relationship, i.e. execute a transaction.

4.2 Subsequent risk determination

In the context of ongoing monitoring of the business relationship with a customer, the reporting entity shall verify again the appropriateness of the initial risk assessment of the customer or a business relationship, and where it proves necessary, the reporting entity shall make a new risk assessment (i.e. perform subsequent risk determination). The reporting entity shall also verify again the appropriateness of the initial risk assessment of a customer or a business relationship in the following cases:

1 in case of a substantial change in the circumstances on which the risk assessment of an individual customer or a business relationship was based, i.e. in case of change in the circumstances that influenced substantially the classification of a customer or a business relationship into an individual risk category;

2 in case where the reporting entity suspects the veracity of data on the basis of which it made a risk assessment of an individual customer or a business relationship.

5 Criteria for determining customer risk categories

In making a risk assessment of an individual customer, business relationship, product or transaction, the reporting entity shall take into account the following criteria:

1 customer type, business profile and structure;

2 geographic origin of the customer;

3 the nature of the business relationship, product or transaction; and

4 the reporting entity's previous experience with an individual customer.

In addition to the criteria listed in the previous paragraph, when determining a degree of risk posed by a customer, business relationship, product or transaction, the reporting entity may also take into account other criteria, such as:

1 the size, structure and business activity of the reporting entity, including the scope, structure and complexity of the business operations conducted by the reporting entity on the market;

2 customer status and ownership structure;

3 customer presence/absence when entering into a business relationship or executing a transaction;

4 the source of funds that are the subject of the business relationship or transaction in case of a customer that, under the criteria prescribed the Act, is a politically exposed person;

5 the intention to enter into a business relationship or to execute a transaction;

6 customer's familiarity with the product and customer's experience and knowledge in this area;

7 other information that shows that a customer, business relationship, product or transaction might involve a higher risk.

6 Customer risk categories

According to risk criteria, a customer, business relationship, product or transaction may be classified into three main exposure categories. They are:

1 high risk,

2 medium (average) risk, and

3 negligible risk.

6.1 High risk of money laundering or terrorist financing

6.1.1 Customer type, business profile and structure

Customers that pose a high risk of money laundering or terrorist financing include:

1 customers (natural or legal persons and other entities) on the list of persons against which the United Nations Security Council (hereinafter: UN Security Council) or the European Union (hereinafter: the EU) have taken measures. These measures include financial sanctions such as the freezing of assets in the accounts and /or ban on the use of assets (economic sources), arms embargo that implies ban on the sale of weapons to the customer, etc.;

2 customers with a residence or a seat in entities which are not subject to international law, or which are not internationally recognised as states (such entities enable fictitious registration of legal persons, issuing of fictitious identification documents, etc.).

The customers that pose a high risk of money laundering or terrorist financing also include:

in the case of natural persons:

a) a customer who is a foreign politically exposed person, i.e. a person that holds or held in the previous year (or longer) a prominent public function and that has a permanent residence in an EU-Member State or in a third country, i.e. a person that holds or held in the previous year (or longer) a prominent public function in an EU-Member State or in a third country, in particular:

1 head of states, heads of governments, ministers and their deputies;

2 elected representatives of legislative bodies;

3 judges of supreme, constitutional and other high courts against whose verdicts, save for exceptional cases, legal remedies may not be applied;

4 judges of financial courts and members of central bank councils;

5 foreign ambassadors, consuls and high-ranking officers of armed forces;

6 members of management and supervisory boards in state-owned or majority state-owned legal persons;

b) a customer whose family member is a foreign politically exposed person such as a spouse or a common-law partner, parents, siblings, children and their spouses or common-law partners;

c) a customer whose associate is a politically exposed person, i.e. any natural person sharing common profits from property or an established business relationship or that has any other close business contacts with the politically exposed person;

d) a customer is not personally present with the reporting entity during a client determination and verification procedure (personal presence with the reporting entity implies that the customer or its legal representative or a person authorised by power of attorney in case where a legal person is represented, is personally physically present with the reporting entity at presentation of a valid personal document on the basis of which the reporting entity verifies the customer's identity);

in the case of legal persons:

a) a customer that is a foreign legal person that does not perform or is not allowed to perform trading, production or other activities in the domicile country of registration (a legal person having a seat in a country known as an offshore financial centre that is subject to certain restrictions as regards direct conduct of a registered activity in that country);

b) a customer is a foreign legal person that performs the activities referred to in Article 3, item 21 of the Act, and that has unknown or hidden owners, secret investors or managers;

c) a customer has a complex status structure or a complex chain of ownership (a complex ownership structure or a complex chain of ownership makes it difficult or prevents identification of the customer's beneficial owner or the person that indirectly ensures funds and thus oversees, directs or in any other way significantly impacts financing and business decisions of the management board or the management of the customer);

d) a customer is a financial organisation that does not need to be licensed by adequate supervisory body to conduct its activities. More specifically, under its home country legislation, the customer is not subject to measures aimed at detecting and preventing money laundering and terrorist financing;

e) a customer is a non-profit organisation (institution, society or other legal person or entity established for charitable public purposes, religious communities, associations, foundations, non-profit associations and other persons that do not perform an economic activity) that meets one of the following conditions:

1 it has a seat in a country known as an offshore financial centre;

2 it has a seat in a country known as a financial or tax haven;

3 it has a seat in a non-EU Member State or in a non-signatory state to the Agreement creating the European Economic Area (hereinafter: the AEEA), i.e. in a country that is not an equivalent third country;

4. any of its members or founders include a natural or a legal person that is a resident of any of the countries mentioned in the previous item;

f) a customer is a legal person established by virtue of issue of bearer shares.

6.1.2 Geographical position of customer

Customers posing a high risk of money laundering and terrorist financing include those with a permanent or a temporary residence or a seat in:

1 a non-EU Member State or a non-signatory state to the AEEA, i.e. in a country that is not an equivalent third country;

2 a country that is, based on an assessment by competent international organisations, known for its narcotics production or well-organised and developed narcotics trafficking (the countries of the Near East, the Middle East or the Far East known for their heroine production: Turkey, Afghanistan, Pakistan and the countries of the Golden Triangle (Myanmar, Laos, Thailand), the countries of South America known for their cocaine production: Peru, Colombia, and the neighbouring countries, the countries of the Middle East, Far East and Central America, known for their production of Indian hemp: Turkey, Lebanon, Afghanistan, Pakistan, Morocco, Tunisia, Nigeria, and the neighbouring countries and Mexico);

3 a country that is, based on an assessment by competent international organisations, known for a high degree of organised crime relating to corruption, arms trafficking, human trafficking or human rights violations;

4 a country that is, based on an assessment by the international organisation Financial Action Task Force, classified as a non-cooperative country or territory (countries or territories that, as assessed by FATF, have no adequate legislation in place in the area of the prevention or detection of money laundering or terrorist financing, no government supervision or no adequate government supervision of financial institutions, countries or territories where the establishment of or the pursuit of the business of financial institutions is possible without authorisation or registration with the competent government authorities, countries which encourage the opening of anonymous accounts or other anonymous financial instruments, countries or territories with weaknesses in the suspicious transactions detection and reporting system, the countries or territories the legislation of which does not recognise the obligation of beneficial owner identification, and whose international cooperation is inefficient or nonexistent);

5 a country subject to the United Nations or EU measures, including in particular complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio, and other means of communication, the severance of diplomatic relations, arms embargo, travel ban, etc.;

6 a country known as a financial or tax haven (such countries enable complete or partial tax remission, or impose taxes at substantially lower rates relative to other countries. Such countries are usually not signatories to agreements on the avoidance of double taxation, or if they are, they do not observe them. The legislation of such countries enables, or requires strict compliance with the obligation of banking and professional secrecy and such countries ensure fast, discreet and cheap financial services. Countries generally known as financial or tax havens include Dubai – Jebel Ali Free Zone, Gibraltar, Hong Kong, Isle of Man, Liechtenstein, Macao, Mauritius, Monaco, Nauru, Nevis Island, Norfolk Island, Panama, Samoa, San Marino, Sark, Seychelles, Saint Christopher and Nevis, St. Vincent and the Grenadines, Switzerland, the cantons of Vaud and Zug, Turks and Caicos Islands, United States of America - federal states of Delaware and Wyoming, Uruguay, Virgin Islands and Vanuatu);

7 a country generally known as an offshore financial centre (such countries impose restrictions on direct pursuit of registered activities of business entities in the country, ensure a high degree of banking and professional secrecy, provide for liberal control of foreign trade, ensure fast, discreet and cheap financial services and registration of legal persons. These countries are often characterised by lack of legislation in the area of prevention and detection of money laundering and terrorist financing. Countries commonly known as offshore financial centres include: Andorra, Anguilla, Antigua and Barbuda, Aruba, Bahamas, Barbados, Belize, Bermuda, the 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, Liechtenstein, Macao, Madeira (Portugal), Marshall Islands, Mauritius, Monaco, Montserrat, Nauru, Nevada (USA),

Netherlands Antilles, Niue, Palau, Panama, Philippines, Samoa, Seychelles, Saint Christopher and Nevis, St. Lucia, St. Vincent and the Grenadines, Zug (Switzerland), Tonga, Turks and Caicos Islands, Uruguay, Vanuatu and Wyoming (USA).

The reporting entities should regard the following international organisations as competent for monitoring the efficacy of compliance with the implementation of the measures in the area of prevention of money laundering and terrorist financing with the provisions of international standards:

1 the European Central Bank,

2 the Committee on the Prevention of Money Laundering and Terrorist Financing of the European Commission,

3 the Financial Action Task Force (FATF),

4 the International Monetary Fund,

5 the World Bank,

6 the Egmont Group of Financial Intelligence Units,

7 the Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL),

8 the International Organization of Securities Commission (IOSCO),

9 the Committee of European Securities Regulators (CESR),

10 the Committee of European Insurance and Occupational Pensions Supervisors (CEIOPS),

11 the International Association of Insurance Supervisors (IAIS).

6.1.3 Business relationships, products and transactions

Business relationships that may pose a high risk of money laundering and terrorist financing include:

1 business relationships that involve regular or large payments from a customer's account, or with a credit or a financial institution in a non-EU Member State or a non-signatory state to the AEEA, or in a country that is not treated as an equivalent third country, or business relationships that involve large payments to a customer's account opened in a credit or a financial institution in a non-EU Member State, a non-signatory state to the AEEA, or in a country that is not an equivalent third country;

2 business relationships entered into or conducted in its name and for the account of the customer by a custodian foreign credit financial or other fiduciary institution with a seat in a country that is a non-EU Member State, a non-signatory state to the AEEA, or in a country that is not an equivalent third country;

3 business relationships entered into without customer's personal presence with the reporting entity, in relation to which the conditions for simplified customer due diligence have not been met; and

4 business relationships that would be entered into on behalf of a person or an entity that is on the list of persons or entities subject to UN Security Council or EU measures.

Products posing high risk of money laundering and terrorist financing include all bearer negotiable instruments and negotiable instruments issued to the bearer or made out to a fictitious recipient, endorsed without restrictions, or instruments in other forms which permit title transfer after surrender and all other incomplete instruments which, though signed, do not indicate the recipient of the funds.

Transactions that pose a high risk of money laundering and terrorist financing include:

1 transactions intended for persons or entities that are subject to UN Security Council or EU measures;

2 transactions that a customer would perform in the name and for the account of a person or an entity that is subject to UN Security Council or EU measures;

3 payment of funds from the account of the customer, i.e. payment of funds to the account of the customer that is different from the account that the customer has indicated during identification, or from the account the customer normally uses or used to use for business transactions (particularly in case of cross-border transactions);

4 transactions intended for persons with a residence or a seat in a country known as a financial or tax haven;

5 transactions intended for persons with a residence or a seat in a country known as an offshore financial centre; and

6 transactions intended for non-profit organisations with a seat in a country known as an offshore financial centre, a country known as a financial or tax haven or in a country that is a non-EU Member State, a non-signatory state to the AEEA, or a country that is not an equivalent third country.

6.1.4 Previous customer experience of the reporting entity

Customers that, in light of the reporting entity's experience, pose a high risk of money laundering and terrorist financing include:

1 persons in respect of which the Office has requested the reporting entity in the past three years to supply information in accordance with Article 59 of the Act;

2 persons in respect of which the Office has issued an order to the reporting entity in the past three years on temporary termination of a suspicious transaction execution;

3 persons in respect of which the Office has issued to the reporting entity in the past three years an order to exercise ongoing monitoring of the customer's financial operations;

4 persons in respect of which the reporting entity has supplied in the past three years data to the Office because of reasons for suspicion, as regards this person or the transaction that this person was conducting, of money laundering or terrorist financing.

6.2 Medium (average) risk of money laundering and terrorist financing

The reporting entity shall classify in the medium (average) risk category that customer, business relationship, product or transaction that cannot be classified, on the basis of the Guidelines criteria, as a high risk category or a negligible risk category. In such a case, the reporting entity shall conduct regular customer due diligence procedures in accordance with the provisions of the Act.

6.3 Negligible risk of money laundering and terrorist financing

The reporting entity shall treat the following as posing a negligible risk of money laundering or terrorist financing:

1 reporting entities referred to in Article 4, paragraph 2, items 1, 2, 3, 6, 7, 8, 9 and 10 of the Act, i.e.:

- banks, branches of Member States banks, branches of third country banks and Member States banks authorised for the direct provision of banking services in the Republic of Croatia;
- savings banks;
- housing savings banks;

- Croatian Post (Hrvatska Pošta, d.d.)

- investment fund management companies, business units of third country investment funds management companies, investment fund management companies from Member States which have a business unit in the Republic of Croatia, i.e. which are authorised to directly perform fund management business in the territory of the Republic of Croatia and third parties which are allowed, in keeping with the law regulating fund operations, to be entrusted with certain matters by the respective management company;

- pension companies that include pension funds management companies and pension insurance companies;

- companies authorised to do business with financial instruments and branches of foreign companies dealing with financial instruments in the Republic of Croatia;

- insurance companies authorised for the performance of life insurance matters, branches of insurance companies from third countries authorised to perform life insurance matters and insurance companies from Member States which perform life insurance matters directly or via a branch in the Republic of Croatia, or other equivalent institutions provided they have a seat in a Member State or in a third country;

2 state bodies, local and regional self-government bodies, public agencies, public funds, public institutes or chambers;

3 companies whose financial instruments have been accepted for trading and are traded on the stock exchanges or the regulated public market in one or several Member States in line with the provisions in force in the European Union, i.e. companies seated in a third country whose financial instruments have been accepted for trading and are traded on the stock exchanges or the regulated public market in a Member State or third country, under the condition that the third country has disclosure requirements in effect in line with the legal regulations in the European Union;

4 persons referred to in Article 7, paragraph 5 of the Act that pose a negligible risk of money laundering or terrorist financing.

IV CUSTOMER DUE DILIGENCE

1 Regular customer due diligence

1.1 Background

Customer due diligence is a key element of prevention in the system of detection and prevention of money laundering and terrorist financing. The purpose of customer due diligence measures is credible identification and verification of a customer's real identity. Customer due diligence comprises identification and verification of the customer's identity, identification of the beneficial owner of the customer, in case where the customer is a legal person, and data on the purpose and the planned nature of a business relationship or transaction and other data, in accordance with the provisions of Article 8 of the Act.

The reporting entity identifies and verifies the customer's identity based on credible, independent and objective sources (by checking the relevant identification document that is an official personal document, original or a notarised extract from the court or other public register). The reporting entity can identify and verify customer identity in two ways: directly in the personal presence of the customer or his legal representative or other person authorised by power of attorney (only in case where the customer is a legal person) or indirectly, through a third person.

The Act expressly prohibits entering into a business relationship or transaction execution in the case where customer identity cannot be determined or where the reporting entity reasonably suspects the credibility or veracity of data or documentation presented by the customer for identification, and in the case where the customer is not ready or shows no signs of readiness to cooperate with the reporting entity in the determination of true and complete data required by the reporting entity in the

framework of customer due diligence. In such a case, the reporting entity shall not enter into a business relationship and shall terminate the existing business relationship or transaction and inform the Office thereof.

The reporting entity may simplify customer due diligence measures only in cases provided for in Article 14 of the Act. The reporting entities shall comply with the exemptions referred to in Article 14 of the Act in cases where a customer or a transaction gives rise to a suspicion of money laundering or terrorist financing.

The Act rests on the basic assumption that some customers, business relationships, products or transactions pose greater and other smaller risks in respect of possible abuse relative to money laundering or terrorist financing. That is why in some cases the Act prescribes particularly thorough know-your-customer and customer verification procedures while in others it allows that simplified customer verification procedures be used. In addition to regular customer due diligence, the Act prescribes another two different approaches to customer due diligence: enhanced customer due diligence which is applied in case of customers that pose a great risk of money laundering and terrorist financing and simplified customer due diligence that can be applied in case of a negligible risk of money laundering and terrorist financing.

1.2 Obligation of customer due diligence

The reporting entity shall conduct customer due diligence:

1 when establishing a business relationship with a customer (a business relationship is any business or other contractual relationship a customer establishes or enters into with a reporting entity which is related to the performance of reporting entity's business activity, such as for instance agreements for the conduct of investment activities, brokerage agreements, financial instruments management agreements, customer access to investment fund management rules. Transfer to another fund of the same investment fund management company is not treated as entering into a new business relationship);

2 with each transaction equal to or greater than HRK 105,000.00, regardless of whether the transaction is made as a single operation or as several transactions which clearly appear to be linked. Transactions that appear as logically mutually linked include:

- two or more consecutive, mutually separated transactions, totalling together over HRK 105,000.00, which a customer is executing on behalf of a third person for the same purpose;

- two or more transactions, totalling together over HRK 105,000.00, executed by several persons who are related or connected by capital, on behalf of the same third person and for the same purpose;

3 in case of suspicion as to the credibility and veracity of the previously obtained data on the customer or a beneficial owner of the customer;

4 whenever a transaction or a customer gives rise to suspicion of money laundering and terrorist financing, regardless of the transaction value.

2 Enhanced customer due diligence

Where a customer, business relationship, product or transaction are characterised as posing high risk of money laundering and terrorist financing, the reporting entities shall conduct enhanced customer due diligence. Under Article 30 of the Act, the following shall be treated as posing high risk of money laundering and terrorist financing: the establishment of a correspondent relationship with a bank or other similar credit institution with a seat in a third country, the establishment of business relationships with a politically exposed person and instances where the customer is not present in person during identification and identity verification in the course of implementation of customer due diligence measures. The Act defines the scope of enhanced customer due diligence and additional measures to be taken by the reporting entity in the cases listed above.

2.1 Enhanced customer due diligence in case of a foreign politically exposed person

Under the Act, foreign politically exposed persons are defined as all natural persons with permanent residence or habitual residence in a foreign country that act or acted during the previous year (or longer) in a prominent public duty, including members of their immediate family or persons known to be close associates of such persons.

In accordance with the provisions of the Act, a foreign politically exposed person is a high-risk customer. Therefore, the reporting entity shall conduct enhanced customer due diligence in all cases where a person defined in accordance with the Act and the Guidelines as a foreign politically exposed person appears as a customer, prior to entering into a business relationship or executing a transaction.

Enhanced customer due diligence, in addition to customer due diligence measures referred to in Article 8, paragraph 1 of the Act, implies the conduct of the following additional measures:

1 collecting data on the sources of funds and property that are or will be the subject matter of a business relationship or a transaction;

2 obtaining a written approval from the competent superior officer before entering into a business relationship with such a customer;

3 very close monitoring of transactions and other business activities carried out with the reporting entity by the foreign politically exposed person, after entering into a business relationship.

Information on whether an individual is a foreign politically exposed person or not, shall be obtained by the reporting entity on the basis of a written statement, signed and completed by the customer before entering into a business relationship or before executing a transaction. Such a written statement shall be provided in the Croatian and in the English language and the reporting entity shall present it for signing to any customer that is a natural person with a permanent residence in another country. The written statement shall include as a minimum the following data:

1 name, surname, permanent residence, date and place of birth of the customer that is entering into a business relationship or executing a transaction, and the number, type and name of the issuing authority of the valid personal document;

2 a statement indicating whether the customer is, under the criteria of the Act, a politically exposed person or not;

3 information indicating the type of a politically exposed person in question (whether it is a person that acts or acted in the previous year (or longer) in a prominent public function, whether it is a family member of a politically exposed person or a close associate of a politically exposed person);

4 information specifying the time during which the customer performed this function, in case of a person that acts or acted in the previous year (or longer) in a prominent public function in a foreign country;

5 information on the type of public function performed by the customer presently or in the previous year (or longer) (head of state, head of government, ambassador, etc.);

6 information on the type of family connection, where the customer is a family member of a politically exposed person that acts or acted in the previous year (or longer) in a prominent public function in a foreign country;

7 information on the type and form of business cooperation, where the customer is a close associate of a person that acts or acted in the previous year (or longer) in a prominent public function in a foreign country;

8 the provision under which the customer allows the reporting entity, for the purpose of verifying the veracity of data specified in the statement, to check customer data by looking into public or other available data records, and to check them directly with the competent authorities of another

state, with the consulate or embassy of this country in the Republic of Croatia, or with the Ministry of Foreign Affairs of the Republic of Croatia;

9 customer's signature.

In case of suspicion as to the veracity of data obtained on the basis of the statement, the reporting entity may check additionally the obtained data by looking into public records and other data available to it (the reporting entity has to determine on its own to what extent will it consider as credible and relevant for customer due diligence, commercial lists, or databases of politically exposed persons) or it may check the obtained data with the competent government bodies of other states, consulates or embassies of foreign countries in the Republic of Croatia and the Ministry of Foreign Affairs of the Republic of Croatia.

Unlike entering into a business relationship with customers resident abroad, when entering into a business relationship with customers with residence in the Republic of Croatia, the reporting entity does not need to obtain a special statement indicating whether a customer is a politically exposed person, but the reporting entity shall, based on the obtained customer information and publicly available information, decide on its own whether the customer is a politically exposed person.

2.2 Customer's absence

The reporting entity shall conduct customer due diligence in case where the customer or his legal representative is not personally present with the reporting entity during customer identification and verification and entering into a business relationship or where customer identity has been determined or verified by a third person.

In addition to the measures referred to in Article 8, paragraph 1 of the Act, customer due diligence shall also comprise at least one of the following measures:

1 obtaining documents, data or information on the basis of which the reporting entity may check and verify additionally the credibility of identification documents and data used in customer identification and verification (a notarised copy of the personal identification document, current, giro, and foreign currency account cards and passbook account);

2 additional verification of the obtained customer data in public and other available data records;

3 obtaining adequate references from a credit or a financial institution having a contractual business relationship with the customer (e.g. holding an account with such an institution), taking into account the fact that in this case only those institutions that comply with home country anti-money laundering and terrorist financing measures may be treated as credit or financial institutions);

4 additional verification of data and information on the customer with the competent government bodies or other competent supervisory authorities in the country where the customer has its residence or seat;

5 establishing a direct contact with the customer either by phone or by a visit to the customer by an authorised person of the reporting entity at the place of his residence or in his seat.

When entering into a business relationship in the absence of the customer, where the customer's identity has been determined and verified by a third person, the reporting entity shall use the measures for determining whether the third person entrusted with customer due diligence has determined and verified the customer's identity in the presence of the customer.

When entering into a business relationship in the absence of the customer, the reporting entity shall, in accordance with the provisions of the Act, implement measures for determining whether the customer has, prior to executing a transaction, made the first payment crediting the reporting entity and debiting the account that the customer or his legal representative holds, or has opened in its name or in the name of the customer, with one of the following credit institutions:

1 bank seated in the Republic of Croatia authorised by the Croatian National Bank to perform banking services;

2 EU-Member State bank with a branch in the Republic of Croatia, authorised for the direct provision of banking services in the Republic of Croatia;

3 branches of third country banks authorised by the Croatian National Bank;

4 savings bank seated in the Republic of Croatia which provides banking services based on an authorisation of the Croatian National Bank; and

5 bank seated in an EU-Member State, a signatory state to the Agreement creating the European Economic Area or an equivalent third country;

and that the customer has indicated in the relevant statement, in the course of entering into a business relationship.

The reporting entity shall pay particular attention to each risk of money laundering and/or terrorist financing that might arise from new technologies which enable anonymity, such as for instance e-banking, and formulate policies and take measures to prevent the use of new technologies for the purpose of money laundering and terrorist financing. The policies and procedures of the reporting entity for the risk associated with a business relationship or a transaction with customers that are not physically present, shall also be applied in business operations with customers conducted by means of new technologies, in accordance with the provisions of Article 33 of the Act.

2.3 Other high-risk customers

Under Article 30, paragraph 3 of the Act, enhanced customer due diligence measures may be also be used in other cases of high-risk customers, business relationships, products or transactions. The use of the prescribed legislative measures, in accordance with the Guidelines, includes the implementation of the following measures:

1 mandatory prior written approval for entering into such a business relationship or for executing a transaction, issued by a superior officer in the reporting entity;

2 mandatory use of one of the following measures:

a) obtaining documents, data or information, based on which the reporting entity additionally checks and verifies the credibility of identification documents and data used in customer identification and verification;

b) additional verification of the obtained customer data by looking into public and other available data records;

c) obtaining relevant references from a credit or a financial institution having a business relationship with the customer (holding an account with that institution), taking account of the fact that in this case only institutions that comply, in accordance with their home legislation, with the measures for the prevention of money laundering and terrorist financing can be treated as credit or financial institutions (from EU or equivalent third countries);

d) additional customer data and information verification with the competent government bodies or other competent supervisory institutions in the country where the customer has its residence or its seat;

e) establishing a direct contact with the customer, either by phone or by a visit to the customer by an authorised person of the reporting entity at the place of his residence or in his seat.

3 mandatory monitoring of transactions and other business activities that the customer performs with the reporting entity.

3 Simplified customer due diligence

As provided by the Act, the reporting entity may conduct a simplified customer due diligence in case of a negligible risk of money laundering or terrorist financing, transparent or publicly available data on the customer that is a legal person or on its beneficial owner, or in case of appropriate supervision of customer's business operations on a national level. This means that the reporting entity performs customer identification and verification, but the procedure involved is less extensive than in the case of regular or comprehensive customer due diligence. The presence of a legal representative of a legal person or a person authorised by power of attorney to act on behalf of a legal person is not mandatory in identity determination, and neither is the identification of the beneficial owner of the customer.

When the Act permits the reporting entity to conduct a simplified customer due diligence in respect of customers that are reporting entities referred to in Article 4, paragraph 2, items 1, 2, 3, 6, 7, 8, 9 and 10, based on the obtained data on the customer and customer risk assessment in terms of the risk of money laundering and terrorist financing, the reporting entity shall determine whether the customer really meets the conditions and poses, in accordance with the Guidelines, a negligible risk of money laundering and terrorist financing.

The reporting entity shall not enter into a business relationship or execute a transaction before it has established all the facts necessary to determine whether a simplified customer due diligence is warranted. The simplified customer due diligence shall not be allowed in cases where a customer or a transaction raises suspicion of money laundering or terrorist financing, and where a customer has been classified, based on risk assessment, as a high-risk customer.

4 Customer due diligence conducted by a third person

When entering into a business relationship, the reporting entity may entrust the customer due diligence procedure to a third party, provided it checks beforehand whether the third person entrusted with the task of customer due diligence meets all the conditions prescribed by the Act and the subordinate legislation.

The reporting entity shall check whether the third person meets the conditions in one of the following ways:

1 by looking into public or other available data records;

2 by looking into documents and business documentation submitted to the reporting entity by the third person; or

3 by obtaining a written statement from the third person, guaranteeing the reporting entity that it meets the prescribed conditions.

A third person that has conducted customer due diligence instead of the reporting entity, shall be responsible for meeting the conditions prescribed by the Act, including the obligation of suspicious transactions reporting and of keeping data and documentation.

Although a third person has conducted customer due diligence instead of the reporting entity, the reporting entity holds the ultimate responsibility for the implementation of customer due diligence.

V IMPLEMENTATION OF THE MEASURES FOR DETECTION AND PREVENTION OF MONEY LAUNDERING AND TERRORIST FINANCING IN BUSINESS UNITS AND COMPANIES IN WHICH THE REPORTING ENTITY HAS A MAJORITY HOLDING OR A MAJORITY VOTING RIGHT AND WHICH HAVE A SEAT IN A THIRD COUNTRY

The reporting entity shall set up a system of uniform money laundering detection and prevention policy. The reporting entity shall take care that the measures for the detection and prevention of money laundering and terrorist financing prescribed by the Act, such as customer due diligence, suspicious transaction reporting, record-keeping, internal audit, appointment of a person authorised by power of attorney, data retention, and other essential circumstances associated with the detection and prevention of money laundering and terrorist financing also be conducted in the same or similar scope

in business units and companies in which the reporting entity has a majority holding or a majority voting right which have a seat in a third country.

Where the standards for the detection and prevention of money laundering and terrorist financing implemented in the operations of business units and companies in which the reporting entity has a majority holding or a majority voting right are in direct opposition to the legislation of the third country in which that business unit or company has a seat, the reporting entity shall inform the Office thereof and take appropriate measures to deal with the risk of money laundering and terrorist financing, such as:

1 setting up additional internal procedures for the prevention or reduction of the possibility of abuse relative to money laundering or terrorist financing;

2 performing additional internal audit of the business of the reporting entity in all key areas most exposed to the risk of money laundering and terrorist financing;

3 setting up internal mechanisms for risk assessment of individual customers, business relationships, products, transactions, in accordance with the Guidelines;

4 implementing strict customer classification policy according to their risk profile and consistent implementation of the measures adopted on the basis of that policy,

5 additional employee education.

The management board of the reporting entity shall:

- ensure that all business units and companies in which the reporting entity has a majority holding or a majority voting right and which have a seat in a third country and their employees are acquainted with the policy for detecting and preventing money laundering and terrorist financing;

- ensure through heads of business units and companies in which the reporting entity has a majority holding or a majority voting right, that the internal procedures for the detection and prevention of money laundering and terrorist financing, adopted on the basis of the Act and the Guidelines, be incorporated into their business processes to the highest extent possible;

- conduct ongoing supervision of adequate and efficient implementation of the measures for the detection and prevention of money laundering and terrorist financing in business units and companies in which the reporting entity has a majority holding or a majority voting right and which have a seat in a third country.

The business units and companies in which the reporting entity has a majority holding or a majority voting right and which have a seat in a third country shall, at least once a year, inform the reporting entity about the measures adopted in the area of detection and prevention of money laundering, particularly about customer due diligence measures, risk analysis/assessment procedures, suspicious transactions detection and reporting, safety and archiving of data and documentation, keeping records on the customer, business relationships and transactions.

VI CUSTOMER BUSINESS ACTIVITIES MONITORING

1 The purpose of monitoring customer business activities

Ongoing monitoring of the business activities of the customer is essential for the determination of the efficacy of implementation of the prescribed measures in the area of detection and prevention of money laundering and terrorist financing. The purpose of monitoring customer business activities lies in the determination of the legitimacy of customer's business operations and verification of the compliance of customer's business operations against the envisaged nature and purpose of the business relationship that the customer has entered into with the reporting entity and against the usual scope of its operations. Monitoring customer business activities can be divided into four segments of the customer's business operations with the reporting entity:

1 monitoring and verifying the compliance of the customer's business operations against the envisaged nature and purpose of the business relationship;

2 monitoring and verifying the compliance of the customer's sources of funds against the envisaged source of funds indicated by the customer during the establishment of a business relationship with the reporting entity;

3 monitoring and verifying the compliance of the customer's business operations against the usual scope of its operations;

4 monitoring and updating the collected customer documents and data.

2 Measures for monitoring customer business activities

1 To monitor and verify the compliance of the customer's business operations against the envisaged nature and purpose of the business relationship that a customer has entered into with the reporting entity, the following measures will be used:

a. an analysis of data on the purchase and/or sale of a financial instrument or an analysis of other transactions during a certain period of time with a view to determining any circumstances that might, in connection with a certain purchase or sale of financial instruments or other transaction, give rise to the suspicion of money laundering or terrorist financing. A decision on suspicion shall be based on the criteria of suspicion determined in the Indicators for the detection of suspicious customers and transactions that give rise to the suspicion of money laundering and/or terrorist financing;

b. conducting a new customer risk assessment, or updating the previous customer risk assessment.

2 To monitor and verify the compliance of the customer's business operations against the usual scope of its operations, the following measures shall be taken into account:

a. monitoring the value of the purchase or sale of financial instruments or of other transactions exceeding a certain amount. The reporting entity shall determine on its own the amount above which it will monitor the business operations of a customer. The amount will be determined for each customer separately, in view of the risk category an individual customer belongs to (for efficient implementation of this measure, the reporting entity may set up adequate software support);

b. an analysis of an individual purchase or sale of a financial instrument or of another transaction from the standpoint of suspicion of money laundering and terrorist financing, in case where the sum total of sales or purchases exceeds a certain value. The analysis of a suspicious purchase or sale of financial instruments or of other transactions is based on the criteria of suspicion determined in the Indicators for the detection of suspicious customers and transactions that give rise to the suspicion of money laundering and/or terrorist financing.

3 To monitor and update the collected customer documentation and data:

a. a repeated annual customer due diligence, in accordance with Article 27 of the Act;

b. a repeated customer due diligence in case of doubt as to the credibility of the previously obtained data on the customer or the beneficial owner of the customer (in case of a customer who is a legal person);

c. verification of data on the customer or his legal representative in a court or other public register;

d. verification of the obtained data directly with the customer or his legal representative or person authorised by power of attorney;

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

3. Scope of customer business activities monitoring

The scope and the intensity of customer business activities monitoring depend on the risk assessment of an individual customer, i.e. on the risk category assigned to a customer. Adequate scope of customer business activities monitoring shall imply:

1 in case of a high-risk customer, the reporting entity shall carry out the prescribed measures for monitoring the business activities of a customer that is assessed as a high-risk customer in accordance with the Guidelines at least once a year. High-risk customer business activities monitoring includes the measures specified in items 1.a, 2.a, 2.b and 3.e of this chapter. In case of a high-risk customer, the reporting entity shall conduct the measures of repeated annual customer due diligence regularly at least once a year, in case the conditions prescribed by the Act have been met;

2 in case of a medium (average)-risk customer, the reporting entity shall carry out the prescribed measures for monitoring the business activities of a customer that is assessed as a medium (average)-risk customer in accordance with the Guidelines at least every three (3) years. Medium (average)-risk customer business activities monitoring includes the measures specified in items 1.b, 2.a, 2.b and 3.e of this chapter. In case of a medium (average)-risk customer, the reporting entity shall conduct the measures of repeated annual customer due diligence regularly at least once a year, in case the conditions prescribed by the Act have been met;

3 in case of a customer that poses a negligible risk, the reporting entity shall carry out the prescribed measures for monitoring the business activities of a customer that is assessed as a low-risk customer in accordance with the Guidelines at least every five (5) years. Low-risk customer business activities monitoring includes the measures specified in items 1.b and 3.e of this chapter. In case of a low-risk customer, the reporting entity shall conduct the measures of repeated annual customer due diligence regularly at least once a year, in case the conditions prescribed by the Act have been met.

The implementation of the measures for customer business activities monitoring shall not be required if the customer has not conducted business activities (purchase and sale of financial instruments or other transactions) after having entered into a business relationship, i.e. during the period referred to in items 1, 2 and 3 of this chapter. The measures for customer business activities monitoring, categorised in accordance with the Guidelines, shall in such a case be conducted by the reporting entity with the first next purchase or sale of a financial instrument or other transaction.

In its internal bylaws, the reporting entity may, in accordance with its money laundering and terrorist financing risk management policy, prescribe more frequent monitoring of business activities of individual types of customers than that envisaged under the Guidelines and impose an additional scope of measures for monitoring customer business activities and determining the legitimacy of the customer's business operations.

VII DATA COMMUNICATION

1 Cash transactions reporting

In accordance with the provisions of the Act, the reporting entity shall supply the Office with data on a customer's cash transaction exceeding HRK 200,000.00 immediately upon or at the latest within three days from the execution of the transaction, using the form which is a constituent part of the Ordinance on the obligation to report cash transactions of HRK 200,000.00 or above to the Anti-Money Laundering Office and on the conditions under which the reporting entities are not obligated to report cash transactions of individual customers to the Anti-Money Laundering Office (Official Gazette 1/2009). A cash transaction is each transaction in which a reporting entity receives from or hands over to a customer cash (banknotes and coins) in an amount exceeding HRK 200,000.00, irrespective of the currency in which such cash is received by the reporting entity or handed over to such customer.

In accordance with the above-mentioned Ordinance, reporting entities shall not be obliged to report to

the Office on a customer's cash transaction involving the depositing of daily proceeds from the sale of goods or services to the customer's account with a reporting entity referred to in Article 4 paragraph 2 items 1 and 2 of the Act, unless there is reason for suspicion of money laundering or terrorist financing.

Reporting entities shall also not be obliged to report to the Office on a cash transaction conducted by a customer for which, in accordance with Article 35 paragraph 1 of the Act, simplified due diligence may be performed, unless there is reason for suspicion of money laundering or terrorist financing.

2 Reporting suspicious transactions

2.1 What is a suspicious transaction?

The Act defines a suspicious transaction as a transaction for which the reporting entity and/or a competent body deem that there is reason for suspicion of money laundering or terrorist financing in relation to the transaction or the person conducting the transaction, i.e. a transaction suspected to involve resources from illegal activities. Pursuant to the provisions of the Act, all transactions which are unusual in their nature, scope, complexity or correlation, lack any evident economic or legal basis, diverge from or are inconsistent with the usual and expected transactions of a customer, as well as other circumstances associated with the customer, may be considered as suspicious transactions. Both customer transactions and business relations may be considered as suspicious. The assessment of the degree of suspicion regarding a customer, transaction or a business relation is based on the suspicion criteria, defined by the list of indicators for the detection of suspicious customers and transactions for which there is reason for suspicion of money laundering or terrorist financing. The indicator lists are basic guidelines for the employees/authorised person for the detection of suspicious circumstances related to a customer or a transaction conducted or business relation entered into by a customer. The employees of the reporting entity must therefore be familiar with the indicators in order to use them in their work. The authorised person shall provide any expert assistance to the employees in assessing whether a particular transaction is suspicious.

The employee of the reporting entity establishing that there is a reason for suspicion of money laundering or terrorist financing shall immediately notify thereof the authorised person for the prevention of money laundering or his/her deputy. The reporting entity shall set up a procedure for reporting suspicious transactions between all organisational units and the authorised person, pursuant to the following instructions:

1 to specify in detail the data communication method (by telephone, facsimile, secure electronic mail, etc.);
2 to specify the type of data submitted (data on customers, reasons for suspicion of money laundering, etc.);
3 to specify the method of cooperation of operating units with the authorised person;
4 to specify the course of action to be taken with a customer in the event of a temporary transaction suspension by the Office;
5 to define the role of the reporting entity's responsible person in reporting a suspicious transaction;
6 to prohibit the disclosure of data indicating that data, information or documentation are to be submitted to the Office;
7 to define measures to continue doing business with a customer (temporary suspension of business, termination of the business relation, conducting enhanced customer due diligence and enhanced scrutiny in monitoring the clients' future business activities, etc.).

2.2 Reporting to the Office

In accordance with the Act, the reporting entity shall submit the required data to the Office in all instances when there is a reason for suspicion of money laundering or terrorist financing. The obligation to report on suspicious transactions shall apply not only with regard to the transactions concluded by a customer, but also with regard to all the transactions that a customer intended/attempted to conclude and then cancelled without any justifiable grounds. The reporting obligation shall apply in the event when the reporting entity, when entering into a business relation or executing a transaction, is unable to identify the customer and verify the customer's identity in the manner prescribed by the Act, i.e. in the event when it is unable to identify the beneficial owner of the customer or obtain data on the purpose and intended nature of the business relationship or transaction, and other data prescribed by the Act and Ordinance on the obligation to report suspicious transactions and persons to the Anti-Money Laundering Office (Official Gazette 1/2009).

The suspicious transaction report shall be submitted to the Office as a rule before the execution of a transaction (by telephone, facsimile or in any other appropriate manner), and shall indicate the deadline for completing the transaction. In the event of preliminary reporting, the reporting entity may submit the report to the Office by facsimile or telephone, but it must also send it in writing, no later than next business day. The reporting entity is often prevented from following the prescribed procedure due to the nature of the transaction, because it has not been executed, or for other justified reasons. In such an event, the reporting entity shall undertake to submit data to the Office at the soonest possible occasion, i.e. immediately upon learning of a reason for suspicion of money laundering or terrorist financing. The reporting entity's report shall indicate the reason for which the reporting entity failed to follow the prescribed procedure.

VIII EDUCATION AND PROFESSIONAL TRAINING

In accordance with the provisions of Article 49 of the Act, the reporting entity shall provide for regular professional training and education of all employees carrying out tasks related to the prevention and detection of money laundering and terrorist financing, that is, of all employees carrying out specific tasks at the workplaces which are or may be indirectly or directly exposed to a money laundering or terrorist financing risk, and of all external collaborators and representatives contractually entrusted with carrying out such tasks, unless they are independent reporting entities for the implementation of measures related to the detection and prevention of money laundering and terrorist financing, in accordance with Article 4 of the Act.

The human resources department of the reporting entity shall, in cooperation with the authorised person, each calendar year and no later than by the end of the current year, draw up an annual professional training and education programme for the prevention and detection of money laundering and terrorist financing. The programme shall set out:

1 the content and scope of the education programme,
2 the aim of the education programme,
3 the education programme implementation method (lectures, workshops, exercises, etc.),
4 the education programme target employee group,
5 the education programme duration.

The reporting entity shall also include all new employees in the education and professional training programmes. The reporting entity shall to this end organise a special professional training and education programme for the prevention and detection of money laundering and terrorist financing. The programme shall at a minimum comprise the following: the provisions on the obligation to conduct customer due diligence and to make a money laundering and terrorist financing risk assessment, the obligation to submit the required data to the Office, the indicators for the detection of customers and transactions in respect of which there is a reason for suspicion of money laundering or

terrorist financing, the requirements related to the protection and retention of data, and the procedures implemented by the reporting entity (ordinances and instructions) for the purpose of implementing the Act, subordinate legislation and Guidelines.

Regular professional training and education within a reporting entity may be performed by the authorised person, his/her deputy or another professionally trained person, appointed on a proposal from the authorised person by the management board of the reporting entity.

IX INTERNAL AUDIT

The reporting entity shall establish regular, systematic and independent control of the regularity and efficiency of application of the prescribed measures for the detection and prevention of money laundering and terrorist financing. The purpose of internal audit is to detect and eliminate irregularities in the application of the prescribed measures for the detection and prevention of money laundering and to improve the system of detection of customers' transactions in respect of which there is a reason for suspicion of money laundering or terrorist financing. When performing internal audit, the reporting entity should give consideration to the following key areas:

1 the performance of operational procedures for the detection and prevention of money laundering and terrorist financing in accordance with the money laundering and terrorist financing risk management policy;
2 the compliance of risk assessment procedures performed in relation to a customer, business relationship, product or transaction with the money laundering and terrorist financing risk management policy and risk analysis;
3 an adequate protection of the submitted data;
4 an adequate and thorough professional training and education for the detection and prevention of money laundering and terrorist financing;
5 an adequate and frequent use of the list of indicators for the detection of suspicious transactions;
6 an adequate and efficient system for the submission of data on the customers and transactions in respect of which there is a reason for suspicion of money laundering or terrorist financing;
7 adequate measures and recommendations for the reporting entity, deriving from internal audit findings.

When performing internal audit, the reporting entity shall also establish control of the regularity and efficiency of application of the measures for the detection and prevention of money laundering and terrorist financing by external collaborators and representatives contractually authorised to perform part of the operations.

The reporting entity shall authorise the internal audit department or another competent supervisory body to independently verify the compliance of the system for detecting and preventing money laundering and terrorist financing with the provisions of the Act, subordinate legislation and Guidelines, which is to notify the management board of the reporting entity of its findings in the form of proposed measures and recommendations for the elimination of irregularities. The reporting entities should control the regularity and efficiency of the application of the prescribed measures for the detection and prevention of money laundering and terrorist financing through regular or extraordinary examinations.

X DATA PROTECTION

The reporting entity shall consider data which it receives and uses pursuant to the provisions of the Act as a business secret, in accordance with the act regulating data secrecy, where such data are so classified by the Office. All employees and other persons having access to such data in any other manner shall ensure the secrecy thereof.

Notwithstanding the above, the following data shall be considered as a business secret or as secret data pursuant to the Act (data which reporting entities are not allowed to disclose to a customer or third person):

1 data indicating that there is reason for suspicion of money laundering or terrorist financing in relation to a customer or transaction, and that these data have been forwarded to the Office;
2 data on the temporary suspension of a suspicious transaction, and all the related details;
3 data on the order to exercise ongoing monitoring of a customer's financial operations;
4 data indicating that an investigation has been or is likely to be initiated against a customer or third party related to money laundering or terrorist financing.

The obligation of data secrecy shall not apply in the case where such data are needed to establish facts in a criminal procedure, where the submission of such data is requested in writing or ordered by a competent court, or where such data are required from the reporting entity by the Office or Agency for the purpose of conducting supervision over the implementation of the Act.

The exemption from the obligation of data secrecy shall also apply in the case where a reporting entity is required pursuant to the Act to submit data to the Office. In doing so, the employees of the reporting entity may not be held accountable for any damage caused to customers or third persons if they act in accordance with the request of the Office, or in the cases set forth in Article 76 of the Act.

Access to data classified as a business secret or as secret shall be restricted. The reporting entity shall in its internal bylaws specify in detail the conditions for and manner of access to such data, taking into account the following instructions:

1 data and documentation shall be stored in such a manner and form as to prevent any unauthorised persons from accessing them and learning of their content (in file rooms meeting technical and safety standards, in locked fire-resistant cupboards, etc.);
2 the members of the management and supervisory boards of the reporting entity, authorised person for the prevention of money laundering and terrorist financing, his/her deputies, heads of the operational units of the reporting entity and other persons appointed by the management board of the reporting entity shall have the right to examine data on customers and transactions in respect of which there is reason for suspicion of money laundering and terrorist financing;
3 it is forbidden to photocopy, copy, alter, publish or in any other manner reproduce the documentation containing such data prior to the written approval of the responsible person;
4 where documentation is photocopied, the reporting entity shall ensure that each photocopy clearly shows which part of the documentation it is made from, that it is clearly labelled as a photocopy, with an indication of the number of photocopies made, the date they were made and the signature of the person who made them;
5 the employees of the reporting entity shall consistently apply personal password login and logout procedures when commencing and ending data processing, thus preventing unauthorised persons from gaining access to the documents;
6 a system shall be in place for monitoring the access to and processing of data and documentation;
7 data shall only be forwarded in such a form as to prevent unauthorised persons from gaining access thereto, by an in-house courier service or by registered mail in a sealed envelope, with a return receipt, etc.; where data are submitted electronically, by means of a safe electronic operating system (message encryption or encoding, etc.);
8 the employees of the reporting entity shall consistently obey the laws regulating personal data protection and data secrecy.

XI AUTHORISED PERSON FOR THE PREVENTION OF MONEY LAUNDERING AND TERRORIST FINANCING

The reporting entity shall appoint an authorised person and one or more deputies to perform money laundering and terrorist financing detection and prevention matters, as laid down in the Act and subordinate legislation. The reporting entity shall ensure that in performing the matters referred to in the Act the authorised person complies with the following instructions:

1 to provide expert assistance to the employees in the operational implementation of measures in the field of money laundering and terrorist financing detection and prevention;

2 to provide advice to the management board of the reporting entity on designing the money laundering and terrorist financing risk management policy;

3 to continuously inform the management board of the reporting entity on the activities performed by the reporting entity in the field of detection and prevention of money laundering and terrorist financing;

4 to cooperate with other reporting entities in designing a uniform money laundering and terrorist financing detection and prevention policy.

XII LEGAL NATURE AND VALIDITY OF THE GUIDELINES

The Guidelines shall be issued pursuant to Article 88 of the Act and shall be binding for all reporting entities set forth in items 7, 8, 9, 10, 15.a (factoring), 15.b, 15.h. and 15.i of the Act. The Agency may, pursuant Article 85 of the Act, verify the compliance of the reporting entity's internal procedures pertinent to money laundering and terrorist financing prevention and detection with the provisions of the Act.

The reporting entities shall at the latest until 15 September 2009 bring their operations into compliance with the content of the Guidelines and ensure the compliance of their internal bylaws, in accordance with the provisions of the Act.

The Guidelines shall enter into force and begin to apply on 15 September 2009.

Class: 011-02/09-04/36
Reg. No: 326-01-09-2
Zagreb, 10 September 2009

Chairman of the Board
Ante Samodol

Appendix I Croatian and International Regulations in the Field of Money Laundering and Terrorist Financing Prevention

1 Anti-Money Laundering and Terrorist Financing Act (Official Gazette 87/08),

2 Ordinance on the obligation to report suspicious transactions and persons to the Anti-Money Laundering Office (Official Gazette 1/09),

3 Ordinance on the obligation to report cash transactions of HRK 200,000.00 or above to the Anti-Money Laundering Office and on the conditions under which the reporting entities are not obligated to report cash transactions of individual customers to the Anti-Money Laundering Office (Official Gazette 1/09),

4 Ordinance on the control of domestic and foreign currency cash taken in and out of the country across the state borders (Official Gazette 1/09),

5 Ordinance on the manner and the time limits for reporting suspicious transactions and persons to the Anti-Money Laundering Office and on the keeping of records by lawyers, law firms, public notaries, audit firms and independent auditors and legal and natural persons engaged in accounting and tax counselling activities (Official Gazette 1/09),

6 Ordinance on the content and type of data on the payer accompanying electronic funds transfer, the obligations of payment services provider and on exemptions from the obligation to collect data in funds transfer (Official Gazette 1/09),

7 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,

8 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,

9 Regulation (EC) No 1781/2006 of the European Parliament and of the Council of 15 November 2006 on information on the payer accompanying transfers of funds,

10 Regulation (EC) No 1889/2005 of the European Parliament and of the Council of 26 October 2005 on controls of cash entering or leaving the Community,

11 Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism, Warsaw, 16 May 2005,

12 40 FATF Recommendations for the prevention of money laundering, June 2003,

13 European Convention on the Suppression of Terrorism, Strasbourg, 27 January 1977, signed by the Republic of Croatia on 7 November 2001 and ratified on 19 September 2002,

14 Protocol amending the European Convention on the Suppression of Terrorism, Strasbourg, 15 May 2003,

15 UN Security Council Resolution 1373, 2001,

16 International Convention for the Suppression of the Financing of Terrorism, New York, 9 December 1999, under ratification in the Republic of Croatia,

17 Council of Europe Convention on the Prevention of Terrorism, Warsaw, 16 May 2005,

18 FATF Special Recommendations on Terrorist Financing, October 2001 and October 2004.

Appendix II

Links

2.1 Links to the lists of countries subject to UN Security Council and EU restrictive measures:

http://ec.europa.eu/external_relations/cfsp/sanctions/list/consol-list.htm
http://www.un.org/sc/committees/

2.2 Links to international institutions

http://www.fatf-gafi.org/pages/0,2987,en_32250379_32235720_1_1_1_1_1,00.html
http://www.coe.int/t/dghl/monitoring/moneyval/

ANNEX XXX List of signed Memorandums of Understanding

	YEAR	STATE
1.	2012.	Sint Maartin
2.		Armenia
3.		The Bahamas
4.		Guernsey
5.	2010.	San Marino
6.		Kosovo
7.	2009.	Canada
8.		Russia
9.		United Arab Emirates
10.		Turkey
11.	2008.	USA
12.		Paraguay
13.		Indonesia
14.	2007.	Moldova
15.		Netherlands Antilles
16.		Aruba
17.	2006.	Georgia
18.		Ukraine
19.	2005.	Bosnia and Herzegovina
20.		Montenegro
21.		Poland
22.		Serbia
23.	2004.	Albania
24.	2003.	Australia
25.		Liechtenstein
26.	2002.	Bulgaria
27.		Romania
28.		Israel
29.		Macedonia
30.		Lebanon
31.	2001.	Lithuania
32.		Panama
33.	2000.	Italy
34.	1999.	Belgium
35.		Slovenia
36.		Czech Republic
37.	2008	Regional protocol on combating money laundering and terrorist financing (FIU Croatia (FIU) - Albania FIU - FIU BiH - FIU Montenegro - Serbia FIU - FIU Slovenia)

ANNEX XXXI Information on Court Register concerning legal persons

All registered persons (Art. 24)
1. registration number; 2. company, abbreviated company, and translation of company i.e. name, abbreviated name and translation of name; 3. seat – place and address in Croatia; 4. business activity – activity of the business entity; 5. full name of individual merchant i.e. persons authorised to represent the company, their personal identification number and residence, and for foreigners also number and designation of identity document and country that issued it and way of representation; 6. branch offices; 7. date of submission of complete financial documents stating the accounting period for the year for which it is submitted where is prescribed obligation to publish these reports; 8. recordation; and 9. other prescribed particulars.
All business entities, except for an individual merchant (Art 24 (3))
1. legal organisational form; 2. date of adoption of the founding document (statute, social contracts, Treaty of Establishment, statement on the establishment or other document) and the date and a brief summary of amendments to these acts; 3. the duration of the business entity if it is restricted; 4. statutory changes; 5. reasons for dissolution of the business entity; 6. liquidation; 7. continuation of the business entity; 8. bankruptcy - a bankruptcy court decision; and 9. termination of business entity
Founders and members of the company (Art 24 (5))
All 1. full name; 2. personal identification number; and 3. residence. ***foreigners - natural persons*** 1. number and designation of the personal identification document; and 2. the state that issued documents ***Foreign legal entities*** 1. company name; 2. seat; 3. registration number and personal identification number.
Public limited companies (Art 29)
1. full name, residence and personal identification number: for foreigners also number and designation of identification document and the state that issued it; for legal entities company or name, seat, registration number and personal identification number i.e. corresponding data for foreign legal entities, for each member of the company, 2. change of social contract, company and seat, business activity;

3. the entry of new members into the company;
4. termination of membership in the company;
5. Changes in authorization to represent the company;
6. reasons for dissolution of company; and
7. Dissolution of the company.

Limited partnerships (Art 30)

1. limited partners – full name, residence and personal identification number, and for foreigners number and designation of personal identification document and the state that issued it, and for the legal person or company name, address, registration number and personal identification number, and the corresponding data for the legal entities;
2. increase and decrease of the role of each limited partner;
3. Data entered for a joint stock company;
4. change of authority to represent the company;
5. reasons for dissolution of society;
6. termination of company; and
7. Data entered for limited liability companies.

Joint stock companies (Art 31)

Basic Data

1. share or approved capital, its increase or decrease and the related decisions;
2. Full name of the board members, deputy board members, president and members of the supervisory board of the company i.e. the executive director, president and board members, their place of residence and personal identification numbers, and for foreigners also number and designation of personal identification document and the state which issued it;
3. full name, residence, personal identification number of the sole shareholder for foreigners also number of personal identification document and the state that issued it, and for legal entities company or name, seat, registration number and personal identification number i.e. corresponding data for foreign legal entity, and changes to these details or an indication that the company does not have only one shareholder;
4. continuation of the founding of a company (date of conclusion of the contract and date of the meeting of the General Assembly, which approved it, property or right to be acquired under the contract and compensation given);
5. transfer of the shares of minority shareholders, upon entering the decision on the transfer of shares shall be entered the sole shareholder;
6. venture agreements stating the types of the venture agreements, date it was made, full names i.e. company or names of other contracting party and in the agreement on the transfer of part of the profit, the agreement on the amount of the profit to be transferred, its amendments and the termination of the contract;
7. joining, joining termination and related decisions;
8. status changes (domestic and cross-border merger and the merger, division, transformation) and related decisions;
9. nullity of company;
10. continuation of company;
11. entry of court decisions;
12. transfer of property:
    a. to legal entities of public law with general assembly decision approving the agreement on the transfer of property and indication of the reasons for the dissolution of the company,
    b. to other persons with an indication of the general assembly decision approving the agreement on the transfer of property;
13. abolition of a company;
14. intended mergers and transferring company assets to a corporation or European company (SE) based abroad and the fulfilment of the conditions for the establishment of a planned Holding – SE; and

15. Other information required by law.

Data on increase and decrease of the share capital

1. decision on increasing share capital indicating the amount of which it was increased;
2. increased equity stakes;
3. decision on conditional increase of the share capital with an indication of the amount by which the shares are issued or the grounds on which the amount was calculated, the lowest increase in the amount of capital or basis for determining the amount for which the shares are to be issued or minimum amount for which they are released;
4. decision to increase the approved capital stock, performed increase and the amount after the increase;
5. decision to increase the share capital from the company's assets with an indication of the amount by which the share capital is increased and annual financial report on the basis of which the capital increases;
6. decision to increase the share capital by shares in property and rights without review of capital increase, indicating the date of publication of the decision to increase the share capital;
7. decision about (regular) reduction of the share capital, indicating the amount by which the equity is to be reduced;
8. reduction of the share capital, the amount of reduction and the amount of share capital after the reduction;
9. decision on simplified reduction of share capital, the amount of reduction and a total amount of capital after reduction, indicating the financial year when the capital was decreased;
10. performed simplified reduction of the share capital;
11. decision to reduce the share capital by withdrawal of the shares, the amount of share capital which refers to the withdrawn shares and the share capital after the reduction;
12. decision to decrease (below the lowest amount) and increase the share capital;
13. increase of the share capital; and
    a. 14. other information prescribed by separate laws.

European company (Societas Europaea, SE) (Art 31a)

1. in case of change of the seat to the Republic of Croatia, the current company, the former seat, the name of the register in which the company is entered and the current number of entries in the registry;
2. intended change of seat to another Member State;
3. for the Board members the corresponding function;
4. full name of the deputy chairman of the board, his residence and personal identification number, and for foreigner also number and designation of personal identification documents and the state that issued it, when it is required under Council Regulation (EZ) no. 2157/2001 of 8 October 2001 on the Statute of the European Society - Societas Europea (SE) and the Law on introduction of the European society - Societa Europea (SE) and the European Economic Interest Grouping (EGIU); and
5. Date of submission of the annual financial reports.

Private Limited Liability Company (Art 31c)

Basic data

1. total amount of share capital, approved capital, its increase or decrease and the related decisions;
2. full name of the board members, deputy board members, the president and members of the supervisory board of the company, their residence and personal identification numbers, and for foreigners number and designation of personal identification documents and the state that issued it;
3. Full name, residence, personal identification number of the members of the company, for foreigners the number and designation of personal identification documents and the state that issued it, and for the legal entity company or name, the seat, registration number and personal identification number i.e. corresponding data for foreign legal entity;

4. if for making the statements and receiving documents on behalf of the company is authorised some person his/her address in the R Croatia shall be indicated as well as his/her full name, personal identification number and residence;
5. continuation of establishing a company (date of conclusion of the contract and date of the meeting of the Assembly);
6. venture agreements stating the type of the venture agreements, date when it was made, names i.e. company or name of other contracting party and in the case of the transfer of part of the profit, the agreement on the amount of profit that is transferred, its amendments and the termination of the contract;
7. joining, joining termination and related decisions;
8. status changes (domestic and cross-border merger and the merger, division, transformation) and related decisions and registration;
9. nullity of company;
10. continuation of company; and
11. Other prescribed particulars.

Data on increase and decrease of the share capital

1. decision on the increase of the share capital indicating the amount of which it was increased;
2. increase of the share capital by deposits;
3. decision to increase the approved capital stock, performed increase and the amount after the increase;
4. decision to increase the share capital of the company from the reserves with an indication of the amount by which the share capital is increased;
5. intention of the company to reduce its share capital;
6. reduction of the share capital indicating the amount for which the share capital is reduced and corresponding registration of a decision of the members of the company on modification of the social contract and registration of the modification of the social contract;
7. decision on the simultaneous reduction and increasing of the share capital; and
8. other information required by law.

Economic interest groupings (Art 32)

1. full name, residence, personal identification number of all members of the association, for legal entities company or name, seat, registration number and personal identification number, including any amendments;
2. full name, residence, personal identification number and powers of the board members authorised to represent the Association;
3. date of the agreement on the establishment of the association and its amendments;
4. Provisions of the contract i.e. decisions to admit new members, upon which he/she is released from liability for obligations incurred prior to the his/her admittance to the association;
5. publishing the Association null and void; and
6. Other information required by law.

Cooperatives (Art 35a)

1. total amount of membership fees;
2. First and last name, residence, personal identification number of cooperative managers and authorities in the representation and first and last names, residences and personal identification numbers of members of the supervisory board if the cooperative has got one;
3. responsibility of cooperative members;
4. Date of conclusion of the contract on establishing a cooperative;
5. Date of the inaugural meeting and the decision to adopt rules of the cooperative; and
6. Changes to the entered data, except for the data stated in Item 4 of this article and the related decisions.

Branches (Art 36)

1. Company or name, headquarters, registration number and personal identification number of

founders, and the company or the name and headquarters of branch office; 2. activities of subsidiaries; 3. First and last name, i.e. first and last names, residence and personal identification number of the person at a branch authorized to represent the business branch of the founder, and for foreigners, the number and designation of personal identification documents and an indication of the state that issued it; 4. name and surname of the procurator whose procuration is confined to one or more of its subsidiaries, their residence and personal identification number, and for foreigners the number of their personal identification document and an indication of the state that issued it, and the recall of procuration; 5. termination of the branch; and 6. Deletion of the branch.
Subsidiary of a foreign founder (Art 37 (3))
1. company and founders' headquarters and company headquarters of the branch and if founder registers more branches and the designation "major subsidiary", and for other subsidiaries ordinal number, 2. name of register, or other record where the founder is registered, in addition to data on a state in which the register is kept, date of registration and registration number under which it is registered, and if it is established in a country where there is no such register, the name publicly certified document on the establishment in accordance with regulations of the country where the founder has headquarters, 3. subject of business activity by the founder and the activity of subsidiaries, 4. First and last name, residence, personal identification number, and for foreigners the number of personal identification document and an indication of the state that issued the person authorized to represent the founders and the scope of their authority, 5. If the founder is a company of capital, the amount of basic capital and the amount of paid shares, and if the founder is a person or sole trader, names of persons personally liable for company debts, their place of residence, personal identification number, number and marks of personal identification documents and indication on the state which issued it, 6. First and last name, i.e. names, residence and personal identification number of the person authorized to represent the founder in the business dealings of the branch, and for foreigners, the number and designation of personal identification documents and an indication of the state that issued it, 7. date of the decision on the establishment of the branch, 8. date of delivery of annual financial statements of founders and other financial documents, stating the date of adoption, 9. termination of the branch:
Legal relations (Art 38)
1. Data on the statute, social contract, statement or act of incorporation, cooperative rules and the decision that is recorded in the register according to law, amendments thereto and related decisions are entered, with a note stating the article that is amended, a brief description of the modifications, date of the decision of the body or the persons who passed its brief content. 2. Data on the legal organizational form of the business entity is registered in legal relationships, its changes and other entries related to the status of the business entity, duration and termination of the business entity, inscriptions related to the bankruptcy and liquidation of the subjects of entry, when there is a statutory obligation to prepare and submit financial reports, and other entries proscribed by law. 3. For capital companies, data is registered on the increase and decrease of the basic capital and the related decision, information about status changes of merger, acquisition and sharing, connection and connection termination, conclusion, modification and termination of business contracts, continuation of establishment, nullity and cancellation of company, and with joint stock companies also the transfer of shares belonging to minority shareholders, transfer of assets to the public-law persons and other persons and other regulations stipulated by law.

4. Legal relationships also include registries of bans, restrictions and the abolition of disposing of these limitations, the determination of control over implementation of the reorganization plan and the elimination of supervision, the bankruptcy judge decisions to be entered ex officio, decisions on pronounced sentences, security measures or precautions , submitted law suits and final judgment, stating the name of the court, the number of verdict, the actions and decisions of other bodies, deleting entries and other registries stipulated by law.
5. By virtue of office, information is registered on filed appeals against the decision on registration, the decisions of the appellate court, and the date of publication and date when the decision becomes final.

ANNEX XXXII Statutory basis for Rulebooks issued by the Ministry of Finance

	Rulebooks	Articles in the AML/CFT Law	Sanctions
1.	Rulebook on reporting the Anti-Money Laundering Office on suspicious transactions and persons (O.G. 01/09)	Article 16 paragraph 2	
		Article 42 paragraph 6	**Article 90** On legal persons – a pecuniary penalty ranging from HRK 50,000.00 to HRK 700,000 On members of management board or other legal person's responsible person – a pecuniary penalty ranging from HRK 6,000.00 to HRK 30,000 On a natural person craftsman or a natural person involved in other independent business activity – a pecuniary penalty ranging from HRK 35,000.00 to HRK 450,000
2.	Rulebook on the manner and deadlines for reporting the Anti-Money Laundering Office on suspicious transactions and persons and on keeping records by lawyers, law firms, notaries public, auditing firms and independent auditors as well as legal and natural persons involved in the performance of accounting and tax advisory services (O.G. 01/09)	Article 54 paragraph 3	**Article 97** On a lawyer, a law firm, a notary public, an auditing firm, an independent auditor, as well as a legal and a natural person rendering accounting services or tax advisory services - a pecuniary penalty ranging from HRK 50,000.00 to HRK 300,000 On members of management board or other legal person's responsible person – a pecuniary penalty ranging from HRK 5,000.00 to HRK 20,000
		Article 81 paragraph 6	**Article 92** On legal persons - a pecuniary penalty ranging from HRK 25,000.00 to HRK 400,000 On members of management board or other legal person's responsible person – a pecuniary penalty ranging from HRK 1,500.00 to HRK 8,000 On a natural person craftsman or a natural person involved in other independent business activity – a pecuniary penalty ranging from

			HRK 8,000.00 to HRK 80,000
3.	Rulebook on reporting the Anti-Money Laundering Office on cash transactions equal to or greater than HRK 200,000 and on the conditions under which the reporting entities shall not be obliged to report to AMLO on cash transactions for designated clients (O.G. 01/09)	Article 16 paragraph 2	
		Article 40 paragraph 3	**Article 91** On legal persons - a pecuniary penalty ranging from HRK 40,000.00 to HRK 600,000 On members of management board or other legal person's responsible person – a pecuniary penalty ranging from HRK 3,000.00 to HRK 15,000 On a natural person craftsman or a natural person involved in other independent business activity – a pecuniary penalty ranging from HRK 15,000.00 to HRK 150,000
4.	Rulebook on the content and type of information on payers accompanying wire transfers, on duties of payment service providers and exceptions from the wire transfer data collection obligation (O.G. 01/09)	Article 15 paragraph 2	**Article 90** On legal persons - a pecuniary penalty ranging from HRK 50,000.00 to HRK 700,000 On members of management board or other legal person's responsible person – a pecuniary penalty ranging from HRK 6,000.00 to HRK 30,000 On a natural person craftsman or a natural person involved in other independent business activity – a pecuniary penalty ranging from HRK 35,000.00 to HRK 450,000
5.	Rulebook on controlling domestic or foreign exchange cash carrying across the state border (O.G. 01/09)	Article 74 paragraph 4	
		Article 81 paragraph 6	**Article 92** On legal persons - a pecuniary penalty ranging from HRK 25,000.00 to HRK 400,000 On members of management board or other legal person's responsible person – a pecuniary penalty ranging from HRK 1,500.00 to HRK 8,000

			On a natural person craftsman or a natural person involved in other independent business activity – a pecuniary penalty ranging from HRK 8,000.00 to HRK 80,000
6.	Rulebook on the manner of and deadlines for supplying the Anti-Money Laundering Office with data on the money laundering and terrorist financing criminal offences (O.G. 76/09)	Article 82 paragraph 2	**Article 97** On a lawyer, a law firm, a notary public, an auditing firm, an independent auditor, as well as a legal and a natural person rendering accounting services or tax advisory services - a pecuniary penalty ranging from HRK 25,000.00 to HRK 180,000 On members of management board or other legal person's responsible person – a pecuniary penalty ranging from HRK 5,000.00 to HRK 20,000
7.	Rulebook on the manner of and deadlines for supplying the Anti-Money Laundering Office with data on misdemeanour proceedings (O.G. 76/09)	Article 82 paragraph 3	**Article 97** On a lawyer, a law firm, a notary public, an auditing firm, an independent auditor, as well as a legal and a natural person rendering accounting services or tax advisory services - a pecuniary penalty ranging from HRK 25,000.00 to HRK 180,000 On members of management board or other legal person's responsible person – a pecuniary penalty ranging from HRK 5,000.00 to HRK 20,000
8.	Rulebook on terms and conditions under which the reporting entities under the Anti-Money Laundering and Terrorist Financing Law shall be allowed to entrust the conducting of customer due diligence with third persons (O.G. 76/09)	Article 28 paragraph 6	**Article 90** On legal persons - a pecuniary penalty ranging from HRK 50,000.00 to HRK 700,000 On members of management board or other legal person's responsible person – a pecuniary penalty ranging from HRK 6,000.00 to HRK 30,000 On a natural person craftsman or a natural person involved in other independent business activity – a pecuniary penalty ranging from HRK 35,000.00 to HRK 450,000

			Article 91 On legal persons - a pecuniary penalty ranging from HRK 40,000.00 to HRK 600,000 On members of management board or other legal person's responsible person – a pecuniary penalty ranging from HRK 3,000.00 to HRK 15,000 On a natural person craftsman or a natural person involved in other independent business activity – a pecuniary penalty ranging from HRK 15,000.00 to HRK 150,000
9.	Rulebook on determining conditions under which the reporting entities shall make grouping of customers representing a negligible money laundering or terrorist financing risk (O.G. 76/09)	Article 7 paragraph 5	**Article 90** On legal persons - a pecuniary penalty ranging from HRK 50,000.00 to HRK 700,000 On members of management board or other legal person's responsible person – a pecuniary penalty ranging from HRK 6,000.00 to HRK 30,000 On a natural person craftsman or a natural person involved in other independent business activity – a pecuniary penalty ranging from HRK 35,000.00 to HRK 450,000

ANNEX XXXIII Rulebook on Determining Conditions under which the Reporting Entities shall make Grouping of Customers Representing a Negligible Risk

MINISTRY OF FINANCE

Pursuant to Article 7, paragraph 5 of the Anti Money Laundering and Terrorist Financing Law (Official Gazette Narodne novine, No. 87/08), the Minister of Finance shall hereby pass the

RULEBOOK
on determining conditions under which the reporting entities shall make grouping of customers representing a negligible money laundering or terrorist financing risk

Article 1

This Rulebook shall prescribe conditions under which the reporting entities referred to in Article 4, paragraph 2 of the Anti Money Laundering and Terrorist Financing Law (hereinafter referred to as the Law) shall make grouping of customers representing a negligible money laundering or terrorist financing risk.

Article 2

In the context of this Rulebook, the public authority bodies shall be understood as the state bodies (the bodies of legislative, executive and judiciary branches), the local and regional self-government units' bodies, legal persons with vested public powers and other legal persons with delegated public powers.

Article 3

(1) In pursuance of Article 7, paragraph 5 of the Law, a reporting entity shall be entitled to group public authority bodies referred to in Article 2 of this Rulebook as customers representing a negligible money laundering or terrorist financing risk, providing such a customer shall simultaneously meet the following requirements:

1. the customer shall perform matters that the were legislatively entrusted with it as public authorities, i.e. matters the customer shall be authorised to perform;
2. customer's identity may be reliably verified from publicly available sources;
3. the customer shall perform a publicly known activity, in which the customer, in keeping with a law rendering the customer liable, shall undertake to regularly carry out audits of financial statements.

(2) In pursuance of Article 7, paragraph 5 of the Law, in addition to the public authority bodies referred to in Article 2 of this Rulebook and the customers referred to in Article 35, paragraph 1, items 1 and 3 of the Law, a reporting entity shall be entitled to group the reporting entities referred to in Article 4, paragraph 2, items 4, 5 and 15 b) of the Law as customers representing a negligible money laundering or terrorist financing risk, providing they shall simultaneously meet the following requirements:

1. customer's identity may be reliably verified from publicly available sources;
2. the customer must mandatorily obtain financial service rendering permits, whereas the financial service rendering permit may be withdrawn in case of a failure to meet requirements as prescribed in a law providing for the rendering of financial services;

3. the customer shall be subject to direct onsite supervision by a competent supervisor, which may set supervising measures applying the principle of proportionality, in keeping with the authorities and procedures for conducting onsite supervision to eliminate illegalities and irregularities concerning the implementation of anti money laundering or terrorist financing measures, actions and procedures.

(3) By way of derogation from the provisions contained in paragraphs 1 and 2 of this Article, should a reporting entity know or have suspicion that a customer is associated with money laundering or terrorist financing, the reporting entity shall be obliged to take course of action in adherence with the provisions contained in Article 8, Article 30, paragraph 3 and Article 42 of the Law.

Article 4

This Rulebook shall be published in Narodne novine, and shall enter into force on the date of publication.

CLASS: 470-06/09-140/1
REF. NO.: 513-06-2/027-09-12
Zagreb, 18 June 2009

MINISTER OF FINANCE

Ivan Šuker

ANNEX XXXIV Rulebook on Terms and Conditions under which the Reporting Entities under the Anti-Money Laundering and Terrorist Financing Law shall be allowed to entrust the Conducting of Customer Due Diligence with Third Persons

MINISTRY OF FINANCE

Pursuant to Article 28, paragraph 6 of the Anti Money Laundering and Terrorist Financing Law (Official Gazette Narodne novine, No. 87/08), the Minister of Finance shall hereby pass the

RULEBOOK
on terms and conditions under which the reporting entities under the Anti Money Laundering and Terrorist Financing Law shall be allowed to entrust the conducting of customer due diligence with third persons

Introductory Provisions

Article 1

This Rulebook shall prescribe:

1. who may be a third person;
2. terms and conditions under which the reporting entities shall be allowed to entrust the conducting of customer due diligence with a third person;
3. obtaining data and documentation prescribed by the Anti Money Laundering and Terrorist Financing Law (hereinafter referred to as the Law) from a third person;
4. instances in which a reporting entity shall be disallowed to establish a business relationship;
5. third person obligations;
6. instances in which the reporting entities shall not be permitted to entrust the conducting of customer due diligence with a third person.

Third Persons

Article 2

(1) A third person may be:

1. a reporting entity referred to in Article 4, paragraph 2, items 1, 2, 3, 4, 6, 7, 8, 9 and 10 of the Law;
2. the Financial Agency;
3. a credit institution from a European Union member-state or a state signatory to the European Economic Area Agreement (hereinafter referred to as the member-state) or a member-state branch of the credit institution seated in the Republic of Croatia;
4. investment funds management companies from a member-state or a business unit of an investment funds management company in a member-state seated in the Republic of Croatia;
5. member-state pension companies;
6. companies authorised to do business with financial instruments from member-states or a business unit of companies for doing business with financial instruments in a member-state seated in the Republic of Croatia;
7. member-state insurance companies or a business unit of an insurance company in a member state seated in the Republic of Croatia;
8. a business unit or a subordinate credit institution of a member-state credit institution in a third country, a business unit or a subordinate company of a member-state investment funds management company in a third country, a business unit or a subsidiary of a member-state company authorised to do business with financial instruments in a third country or a business unit or a subordinate insurance company of a member-state insurance company in a third country;

9. credit institutions, investment funds management companies, pension companies, companies authorised to do business with financial instruments, insurance companies, seated in a third country, providing they shall simultaneously meet the following requirements:
   a. they are subject to mandatory registration;
   b. they apply measures of customer due diligence, keeping records and data in agreement with the provisions contained in 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, the recommendations of the Financial Action Task Force (FATF), i.e. equivalent standards, the application of which measures shall be subject to supervision conducted in keeping with the provisions contained in Directive 2005/60/EC or have their business seat in a third country applying measures equal to the provisions contained in Directive 2005/60/EC.

(2) Outsourced associates and agents of a reporting entity who shall conduct customer due diligence on the basis of a contractual relationship shall not be regarded third persons referred to in Article 28, paragraph 1 of the Law, it shall rather be deemed that the reporting entity has conducted customer due diligence in such a case.

(3) A shell bank or another similar credit institution which shall not perform or shall not be allowed to perform its business activity in its country of registration may not be a third person.

Terms and conditions under which the reporting entities may entrust the conducting of customer due diligence with a third person

Article 3

The reporting entities obliged to implement anti money laundering and terrorist financing measures, actions and procedures as set forth in Article 4, paragraph 2 of the Law may entrust the conducting of customer due diligence with a third person under terms and conditions prescribed in Article 28 of the Law and Article 2, paragraph 1 of this Rulebook.

Obtaining data and documentation from a third person

Article 4

(1) A third person who shall conduct customer due diligence as per the provisions of the Law and this Rulebook in lieu of a reporting entity shall be obliged to supply the reporting entity without any undue delay with obtained data on the customer necessary for the reporting entity to establish a business relationship in agreement with the Law.

(2) A third person must supply the reporting entity without any undue delay with a copy of the identification document and other documentation, on the basis of which the third person has conducted customer due diligence and obtained the required customer data. The reporting entity shall keep the obtained copies of documents and documentation in keeping with the provisions of the Law providing for data protection and keeping.

(3) Should the reporting entity judge that there shall be suspicion of the credibility of customer due diligence conducted or documents and other documentation, i.e. of the veracity of the customer data collected, the reporting entity shall immediately require the third person files a written statement on the credibility of customer due diligence conducted and the veracity of customer data collected.

Instances in which reporting entities shall not be allowed to establish a business relationship

Article 5

A reporting entity shall not be allowed to establish a business relationship in instances when:

1. customer due diligence was conducted by a person other than a third person as per Article 2 of this Rulebook;
2. a third person entrusted with the conducting of customer due diligence by the reporting entity has identified the customer and verified customer's identity without customer's presence with the third person;
3. the reporting entity has not received data referred to in Article 4, paragraph 1 of this Rulebook from a third person who conducted customer due diligence;
4. the reporting entity has not received copies of identification documents and other customer documentation referred to in Article 4, paragraph 2 of this Rulebook from a third person who conducted customer due diligence;
5. there shall exist suspicion of the credibility of customer due diligence conducted or the veracity of customer data collected, and the reporting entity, contrary to its request, has not received a written statement from the third person referred to in Article 4, paragraph 3 of this Rulebook or the written statement has not removed suspicion from the credibility of customer due diligence conducted.

Third person obligations

Article 6

Should a third person who conducted customer due diligence in lieu of a reporting entity be a reporting entity provided for in Article 4, paragraph 2, items 1, 2, 3, 4, 6, 7, 8, 9 and 10 of the Law or should it be the Financial Agency, the third person also shall be responsible to meet the requirements as per the Law, including the obligation of reporting transactions and persons in relation to which there shall exist reasons for suspicion of money laundering or terrorist financing, as well as the obligation of keeping data and documentation.

Instances in which reporting entities shall not be permitted to entrust the conducting of customer due diligence with a third person

Article 7

The conducting of customer due diligence may not be entrusted with a third person in the following instances:

1. if the customer shall be a foreign legal person which does not perform or is not allowed to perform trading, production or other activities in its domicile country of registration;
2. if the customer shall be a trust or other similar foreign law company with unknown, i.e. hidden owners, secret investors or managers.

Transitional and Final Provisions

Article 8

This Rulebook shall be published in Narodne novine, and shall enter into force on the date of publication.

CLASS: 470-06/09-140/1
REF. NO.: 513-06-2/027-09-13
Zagreb, 18 June 2009

MINISTER OF FINANCE
Ivan Šuker

ANNEX XXXV Rulebook on the Manner and Deadlines for Reporting on Suspicious Transactions

MINISTRY OF FINANCE

Pursuant to Article 54 and Article 81, paragraph 6 of the Anti-Money Laundering and Terrorist Financing Law (Official Gazette *Narodne novine* No 87/08), the Minister of Finance shall hereby pass the

RULEBOOK

on the manner and deadlines for reporting the Anti-Money Laundering Office on suspicious transactions and persons and on keeping records by lawyers, law firms, notaries public, auditing firms and independent auditors as well as legal and natural persons involved in the performance of accounting and tax advisory services

Background Provisions

Article 1

This Rulebook shall prescribe:
1. the manner and deadlines for reporting the Anti-Money Laundering Office (hereinafter referred to as the Office) on a transaction and a person for which the reporting entity referred to in Article 4, paragraph 2, item 16 (hereinafter reported to as the Reporting Entities) of the Anti-Money Laundering and Terrorist Financing Law (*Narodne novine* No. 87/08; hereinafter referred to as the Law) shall know or have suspicion that they are associated with money laundering or with terrorist financing (hereinafter referred to as a suspicious transaction);
2. the type and manner of keeping records (hereinafter referred to as the records) referred to in Article 81, paragraph 2 of the Law.

Manner of Reporting the Office

Article 2

(1) The Reporting Entities shall report the Office on suspicious transactions and persons in relation to which reasons for suspicion of money laundering or terrorist financing shall exist before the conducting of a suspicious transaction in one of the following manners:
1. by phone,
2. by fax.

(2) Exceptionally, if the Reporting Entity was not in position to notify the Office of the suspicious transaction before its execution due to the nature of the transaction or for other justified reasons, the Reporting Entity shall be obliged to report the Office subsequently and no later than the next business day by fax, registered mail or a courier. The suspicious transaction and person report is to substantiate the reasons for which the Reporting Entity was objectively unable to comply with what was prescribed.
(3) The Reporting Entities shall report the Office on suspicious transactions and persons in relation to which reasons for suspicion of money laundering or terrorist financing shall exist also after the execution of the suspicious transaction no later than the following business day in one of the following manners:
1. by fax;
2. by registered mail;
3. through a courier.

(4) In all instances when a customer shall seek an advice from the Reporting Entities on money laundering or terrorist financing, the Reporting Entities shall notify the Office thereof immediately, and no later than within three business days from the date the customer sought for such an advice.

Form for Reporting the Office

Article 3

(1) The Reporting Entities shall supply the Office with suspicious transactions and persons data and information using the Form for Reporting Suspicious Transactions and Persons by Professional Activities (UZSPN-O-54) which form shall be an integral part of this Rulebook jointly with the enclosed Form and the Form Filling Instructions.
(2) While completing the form, the Reporting Entities shall undertake to adhere to the instructions provided at the back of the form.
(3) Should it happen that incomplete or inaccurate information were sent during the suspicious transactions form filling, the Reporting Entity shall undertake to supply a correctly completed form, with full and accurate information, at an express request of, within the set deadline and in the manner the Office shall define.

Type and Manner of Records Keeping

Article 4

(1) The Reporting Entities shall chronologically keep records on: customers, business relationships and the reported suspicious transaction in such manner that shall enable their efficient supervision by an authorised supervisory body.
(2) The records referred to in paragraph 1 of this Article shall contain the following information: customer's name and surname, type and date of establishing the business relationship, date of conducting or refusal to conduct a transaction, date of seeking an advice in relation to money laundering or terrorist financing and date of reporting the Office.

Transitional and Final Provisions

Article 5

With the effective date of this Rulebook the provisions contained in the Rulebook on the Implementation of the Anti-Money Laundering Law (*Narodne novine* No. 189/03) referring to reporting the Office on suspicious transaction and persons by lawyers, law firms, notaries public, auditing firms, certified auditors, legal or natural persons involved in the performance of accounting or tax advisory services shall discontinue.

Article 6

This Rulebook shall be published in *Narodne novine* and shall enter into force on the date of its publication.

Class: 470-06/07-04/1
Ref. No.: 513-06-2/027-08-81
Zagreb, 19 December 2008

MINISTER OF FINANCE

Ivan Šuker

ANNEX XXXVI STR Reporting Form

RESTRICTED
AFTER COMPLETION

FORM FOR REPORTING THE ANTI-MONEY LAUNDERING OFFICE ON SUSPICIOUS TRANSACTIONS AND PERSONS BY PROFESSIONAL ACTIVITIES

A. CLIENT INFORMATION (COMPLETE THE FORM IN CAPITAL LETTERS)

1	The Client is		☐ Natural person ☐ Natural person - craftsman or a person performing independent activity ☐ Legal person ☐ NGO ☐ Endowment ☐ Foundation ☐ Religious community ☐ Other (please specify):
2	Surname Name	Name of legal person and other entities made equal	
3	Identification No. / Business registration No.		
4	Address / Seat	Street and No. Place State	
5	Date of Birth		DD/MM/YYYY
	Place of Birth		
6	Identification document	Type of document	☐ I.D. Card ☐ Passport ☐ Other (please specify):
		Number of document	
		Name of issuer	

B. INFORMATION ON THE PURPOSE AND INTENDED NATURE OF THE BUSINESS RELATIONSHIP

7	Date of business relationship establishment	DD/MM/YYYY
8	Information on the purpose and intended nature of the business relationship and information on client's business activity	
9	Information on the source of funds which are or will be a subject matter of transaction or business relationship	

C. INFORMATION ON PERSON AUTHORISED BY POWER OF ATTORNEY OR LEGAL REPRESENTATIVE ESTABLISHIN BUSINESS RELATIONSHIP OR CONDUCTING A TRANSACTION ON BEHALF OF A LEGAL PERSON

10	Surname		
	Name		
11	Address	Street and No.	
		Place	
		State	
12	Date of Birth		DD/MM/YYYY
	Place of Birth		

D. INFORMATION ON NATURAL PERSON CLIENT'S BENEFICIAL OWNER (see enclosure to the Form)

13	Surname		
	Name		
14	Address	Street and No.	
		Place	
		State	
15	Date of Birth		DD/MM/YYYY
	Place of Birth		

E. TRANSACTION RECIPIENT - CLIENT TO WHOM TRANSACTION IS INTENDED (see enclosure to the Form)

16	The Client is	☐ Natural person ☐ Natural person - craftsman or a person performing independent activity ☐ Legal person ☐ NGO ☐ Endowment ☐ Foundation ☐ Religious community ☐ Other (please specify):

COPY FOR THE OFFICE / COPY FOR THE REPORTING ENTITY UZSPN-O-54

17	Surname	Name of legal person and othe entities made equal	
	Name		
18	Identification No. / Business registration No.		
19	Address / Seat	Street and No.	
		Place	
		State	

F. SUSPICIOUS TRANSACTION INFORMATION (see enclosure to the Form)

20	Transaction	☐ Executed ☐ Not executed
21	Purpose and manner of transaction execution:	
22	Transaction execution date	DD/MM/YYYY
23	Currency tag	
24	Currency amount	,
25	Value / total value / in HRK	,

G. SUSPICIOUS PERSON INFORMATION (see enclosure to the Form)

26	The person is		☐ Natural person ☐ Natural person - craftsman or a person performing independent activity ☐ Legal person ☐ NGO ☐ Endowment ☐ Foundation ☐ Religious community ☐ Other (please specify):
27	Surname	Name of legal person and othe entities made equal	
	Name		
28	Address / Seat	Street and No.	
		Place	
		State	
29	Date of Birth		DD/MM/YYYY
	Place of Birth		

H. INFORMATION ON REASONS FOR SUSPICION OF MONEY LAUNDERING OR TERRORIST FINANCING

30	Explanation of reasons for suspicion of	☐ MONEY LAUNDERING ☐ TERRORIST FINANCING ☐ Client sought for money laundering or terrorist financing advice
31	Indicator code and name:	
32	Suspicious transaction report already delivered	☐ by phone ☐ by fax ☐ in another way:
	Report delivery date DD/MM/YYYY	

I. REPORTING ENTITY INFORMATION

I.1. NAME

33	Reporting entitiy and the seat	

I.2. PERSON WHO NOTIFIED THE OFFICE

34	Surname and name	
	Signature and completion date DD/MM/YYYY	

COPY FOR THE OFFICE / COPY FOR THE REPORTING ENTITY UZSPN-O-54

ANNEX XXXVII Inter-agency agreements signed by Law Enforcement

1. Joint Declaration on Cooperation between the Ministry of the Interior of the Republic of Croatia and the Ministry of the Interior of the Baden - Württemberg on cooperation and improving standards in all areas of performing police duties (Zagreb, 18/11/1998);
2. Joint Declaration on Cooperation between the Ministry of the Interior of the Republic of Croatia and the Bavarian State Ministry of the Interior in the fight against transnational organized crime, illicit drug trafficking and terrorism (Munich, 28/11/1994) and a new Joint Declaration (Zagreb, 24/05/2000);
3. Joint Declaration between the Ministry of the Interior of the Republic of Croatia and the Bavarian State Ministry of the Interior on international police co-operation, especially in the prevention and fight against organized crime, illicit drug trafficking and terrorism (Kaštela, 08/08/2012);
4. Agreement between the Ministry of the Interior of the Republic of Croatia and the Ministry of the Interior of the Republic of Bulgaria on police cooperation (20/12/2005);
5. Agreement between the Ministry of the Interior of the Republic of Croatia and the Ministry of the Interior of the Republic of Montenegro on police cooperation (Zagreb, 22/11/2005);
6. Agreement on Cooperation between the Ministry of the Interior of the Republic of Croatia and the Ministry of Public Security of the People's Republic of China (Beijing, 26/02/1997);
7. Agreement on Cooperation between the Ministry of the Interior of the Republic of Croatia and the Ministry of the Interior of the Republic of Poland on the prevention and detection of crime, (Warsaw, 08/11/1994);
8. Agreement between the Ministry of the Interior and Federal Service for drug trafficking suppression of the Russian Federation on cooperation in the fight against illicit trafficking of drugs, psychotropic substances and precursors (Zagreb, 07/09/2007)
9. Protocol on bilateral police cooperation of Criminal Police of the Republic of Austria and the Republic of Croatia (Graz, 25/03/1992);
10. Declaration on cooperation between the Ministries of the Interior of the Republic of Croatia and Ukraine (Zagreb, 24/05/1993);
11. Memorandum of Understanding between the Ministry of the Interior of the Republic of Croatia, Croatian National Protection and Rescue Service and the Ministry of the Interior and overseas relationships of the Kingdom of the Netherlands in the field of home affairs (Cannes, 07/07/2008);
12. Memorandum of Understanding between the Republic of Croatia and the United States of America on fight against crime (Zagreb, 16/07/2009);
13. Memorandum of Understanding on cooperation between the Ministry of the Interior of the Republic of Croatia and Ministry of the Interior of the Republic of Kosovo (Priština, 07/10/2009);
14. Agreement on Cooperation between the Ministry of the Interior of the Republic of Croatia and the Ministry of the Interior of the Russian Federation (Istanbul, 23/11/2012).